I·C·S
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy Enhanced Cloud Computing

Institute for Cyber Security Overview

Ravi Sandhu
Executive Director

Professor of Computer Science
Lutcher Brown Chair in Cyber Security

October 2019

ravi.sandhu@utsa.edu
www.ics.utsa.edu
www.profsandhu.com

World-Leading Research with Real-World Impact!

UTSA Computer Science

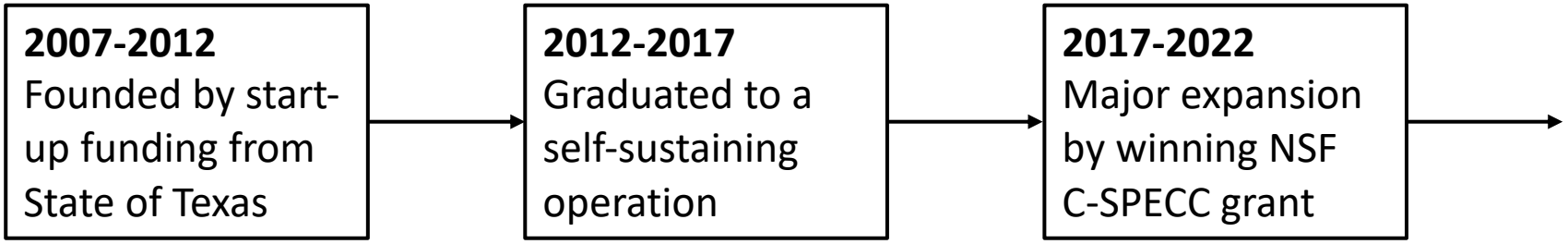
ICS Mission and History

I·C·S The Institute for Cyber Security

C·SPECC Center for Security and Privacy Enhanced Cloud Computing

MISSION

Excellence in graduate-level sponsored research



- **FlexCloud & FlexFarm**
  World class research laboratories
- Sustained production of PhD graduates and sponsored research

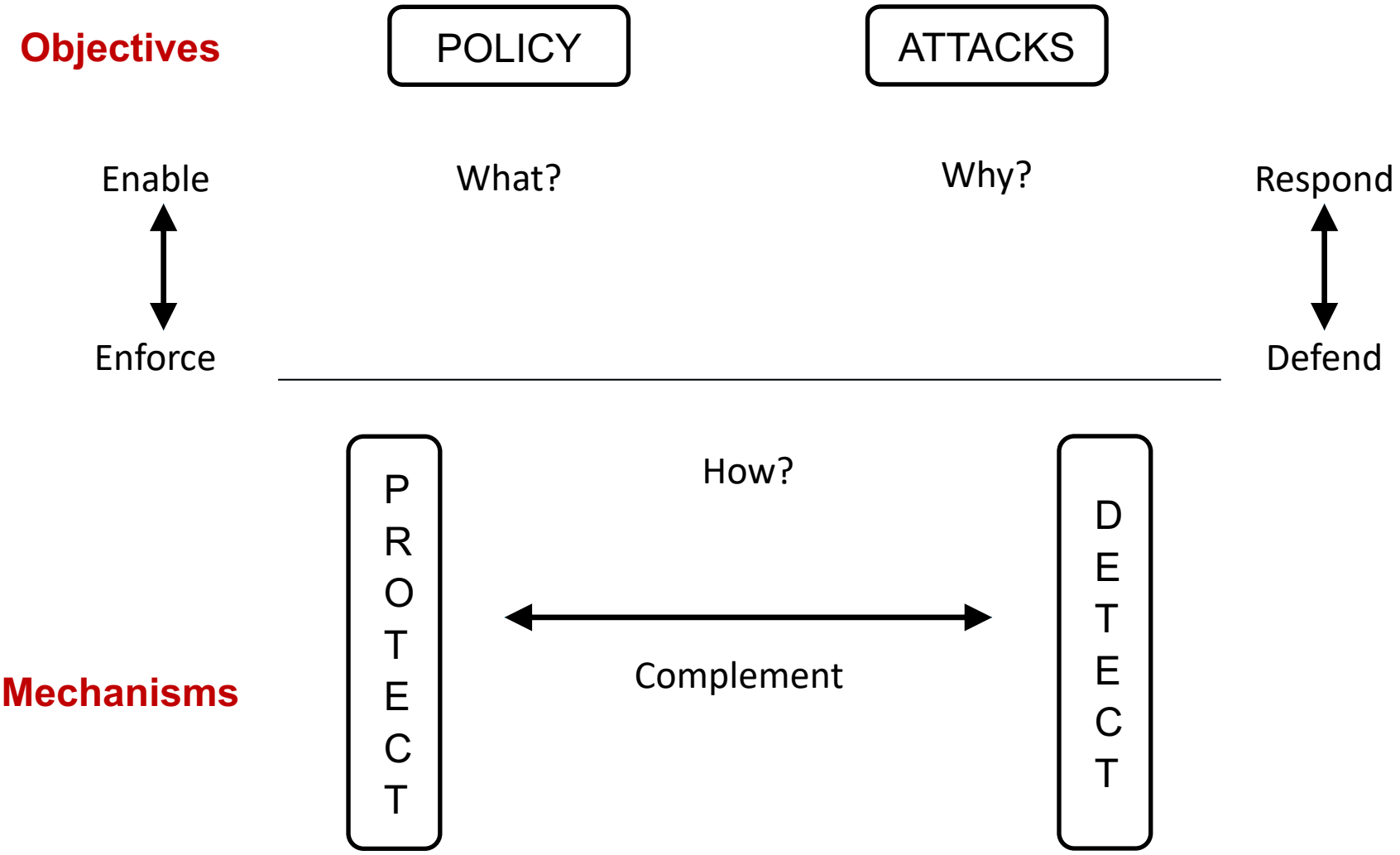
In collaboration with:
College of Engineering
College of Business
College of Education
Open Cloud Institute
Cyber Center for Security & Analytics

Partnership with 4 NISD High Schools:
Harlan, Woodson, Taft, Business Careers

World-Leading Research with Real-World Impact!

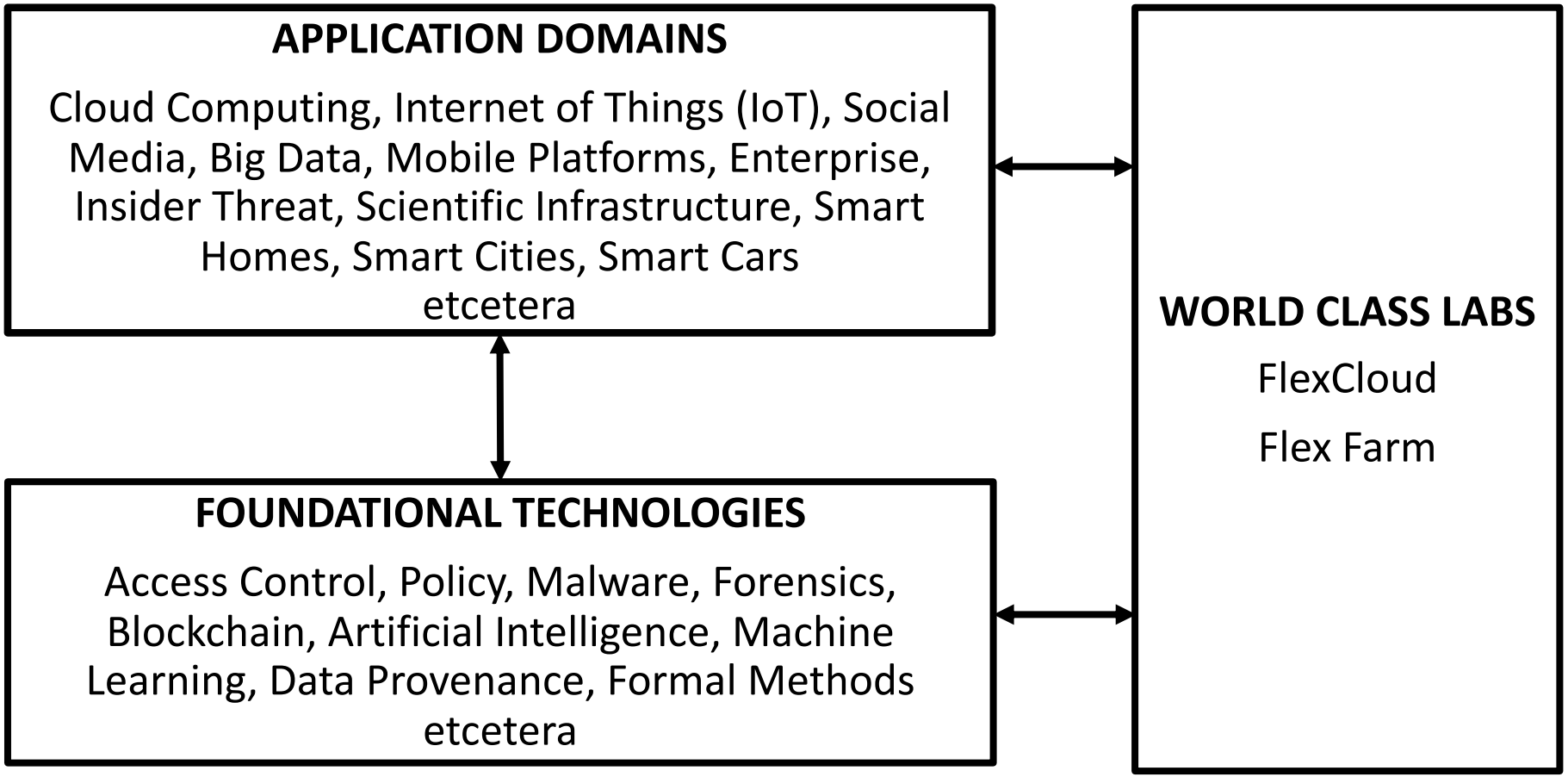
UTSA Computer Science

Holistic Cyber Security Research



Holistic Cyber Security Research

ICS Major Research Thrusts



Goal: Broaden and Deepen

Facts and Figures

PAST SYNOPSIS

- PhDs graduated: 27
- External funding raised: $22M

CURRENT STATUS

- Faculty affiliates: 22
  - College of Sciences: 8
    College of Engineering: 7
    College of Business: 6
    College of Education: 1
- Current PhD students: 29
  - College of Sciences: 19
    College of Engineering: 7
    College of Business: 2
    College of Education: 1
  - Domestic vs Foreign: roughly 50-50

- This slide was intentionally left blank.

Institute for Cyber Security: Galahad Project

James Benson
Technology Research Analyst

October 2019

James.Benson@utsa.edu
www.ics.utsa.edu
https://gitlab.com/utsa-ics/galahad

ICS Data Center

- Research Data Center (RDC) was opened in the summer of 2012.
- Total square footage for servers is 1,632 sq. ft.
- The entire MS RDC is 3,558 sq. ft.

- Our equipment consists of over:
  - 1,300 threads,
  - 10TB of RAM,
  - 370TB of storage, and a
  - 10GB backbone.

Galahad 10,000 Foot

- Galahad was Star Lab's solution for IARPA VirtUE program - Virtuous User Environment (VirtUE).

- 4 Original Contenders:
  - Star Labs;
  - Raytheon BBN;
  - Siege Technologies;
  - and Next Century

- **Galahad is unique** in that it was transitioned from Star Labs to ICS; We have open-sourced it. To create a turn-key opensource deployment tool to share it with others.

Goals and Motivation

- Objective: Detection and mitigation of threats attempting to exploit, collect, and/or effect user computing environments (UCE) within public clouds

- Cloud service providers have not offered any “game changing” security solutions
  - Adversaries can leverage an arsenal of capabilities used to succeed
  - Providers cannot necessarily be trusted

- Current end-point security solutions and analytical approaches are not tuned for cloud environments

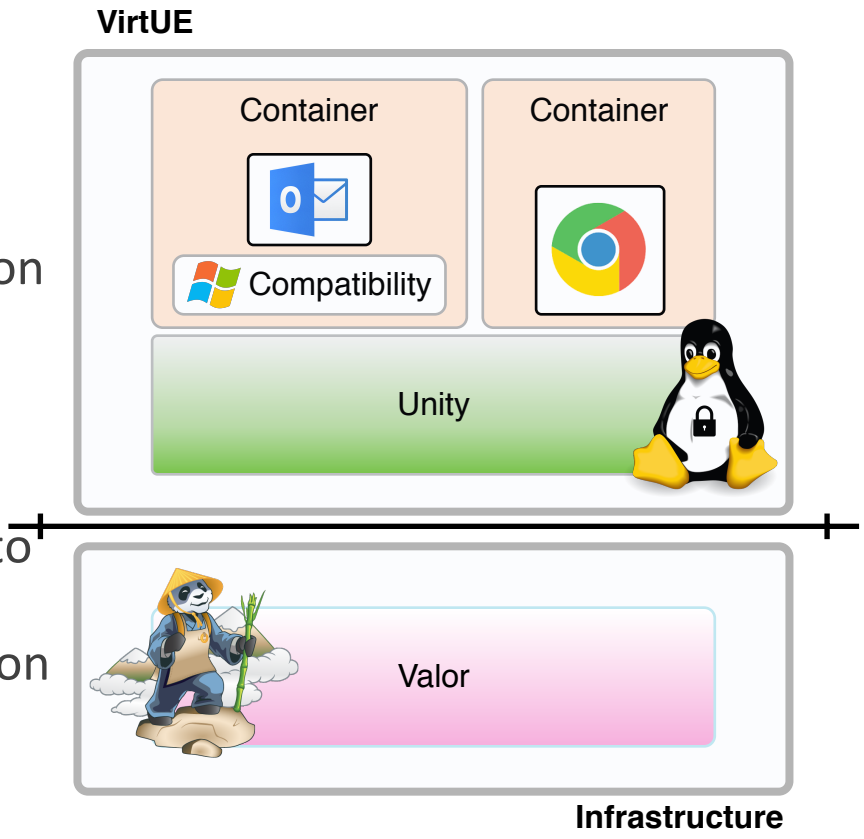
Galahad Approach

- To combat threats in a public cloud, isolate, protect what is controlled, and maneuver
  - Do not attempt to establish trust
  - Do not require special cloud services, e.g., dedicated servers
  - Impede the ability of adversaries to operate within AWS by making it more difficult to co-locate
  - Force adversaries to consume more resources thereby increasing the accuracy, rate, and speed with which threats maybe detected
  - Facilitate the creation of role-enabled security models
  - Reduce attack surface area, hardened kernel, real-time sensing, limit resources.

Galahad VirtUE

Containers for easy packaging and security configuration

A nested hypervisor to facilitate regular, recurring live migration of Unity VMs inside AWS

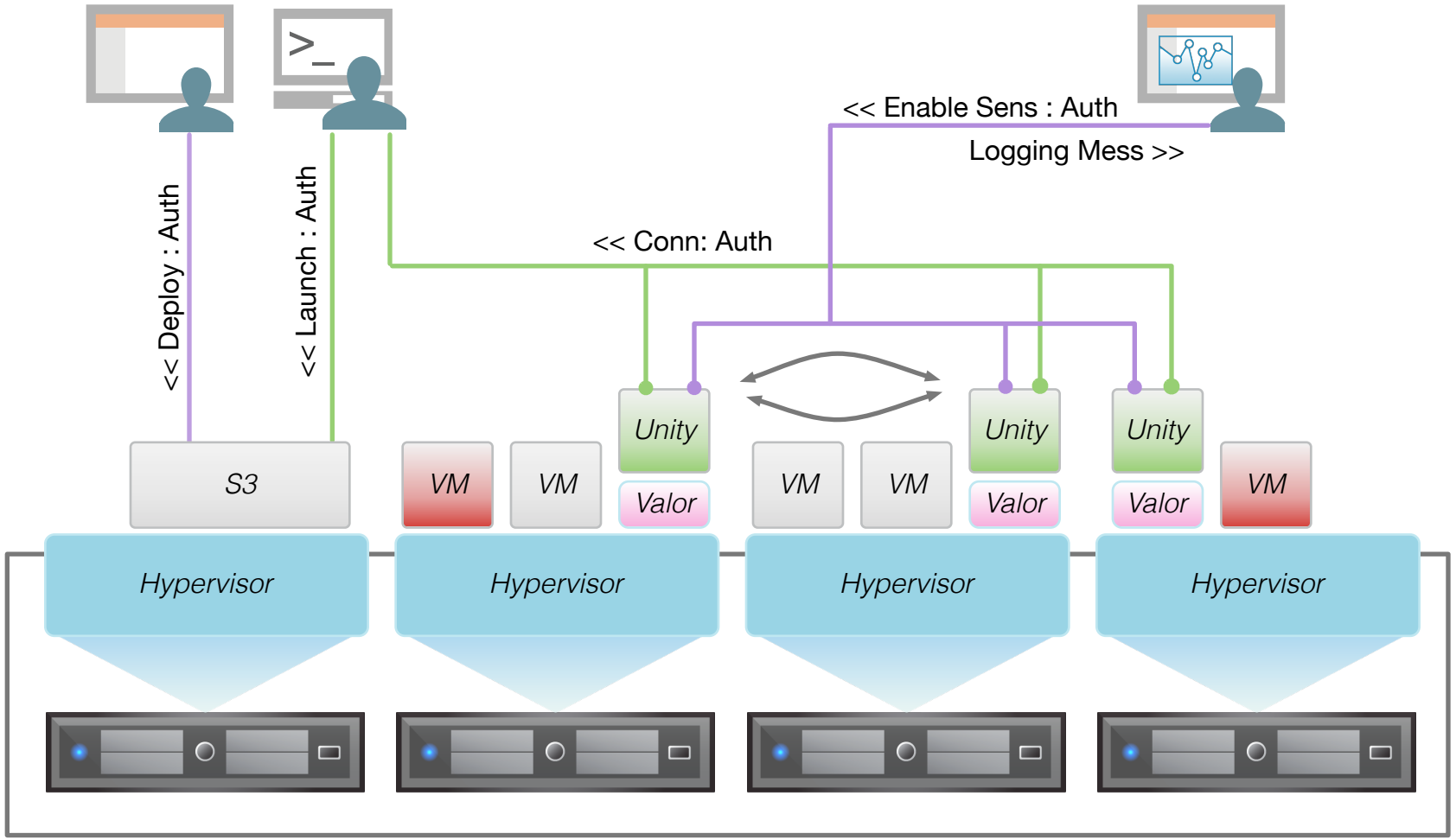


A small, hardened, de-privileged Linux OS VM

Sensing/control Capabilities

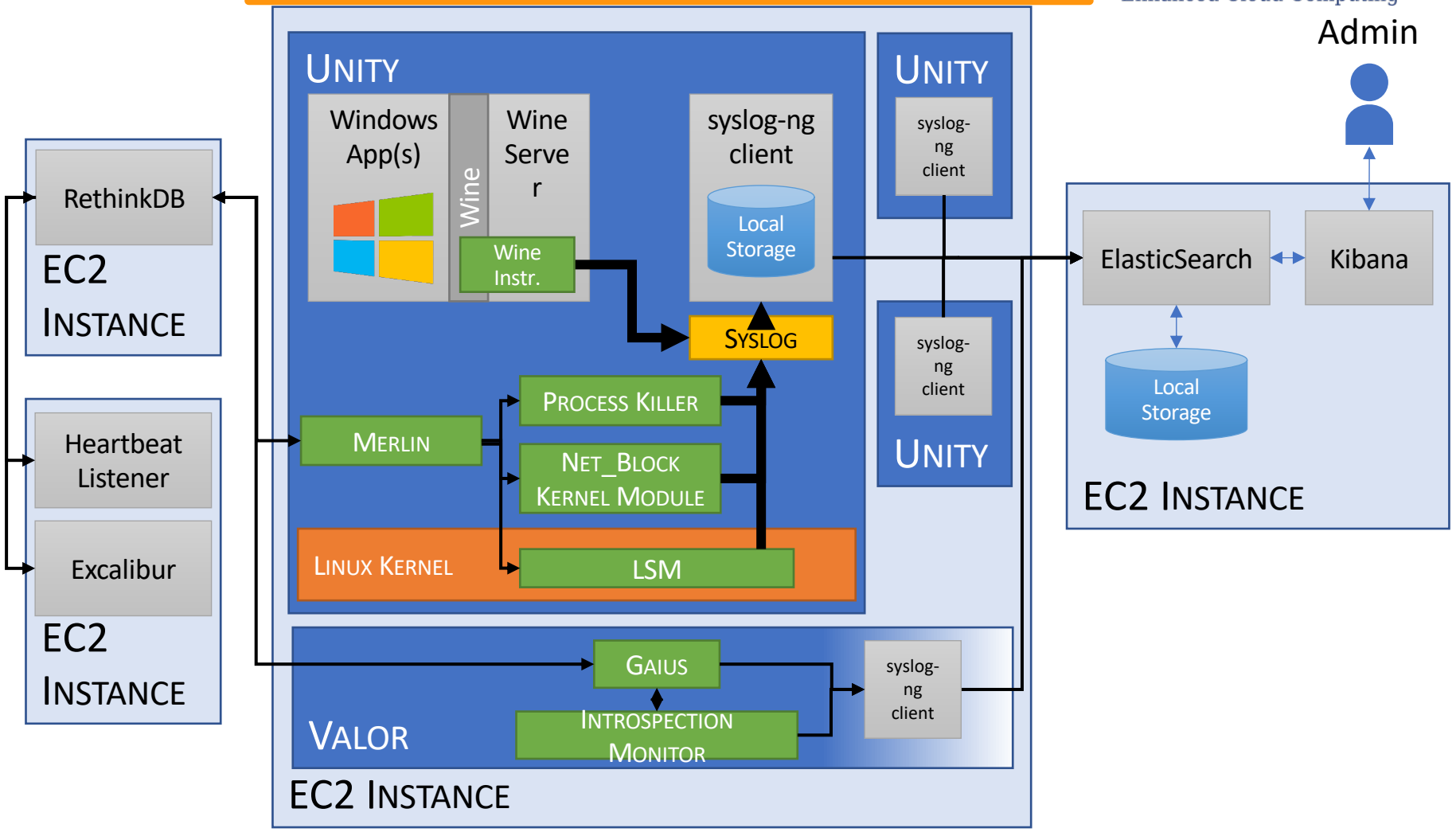
- Valor:
  - Network communications,
  - Virtual memory remapping,
  - Physical device access
- Unity/VirtUE:
  - Process creation,
  - Storage usage,
  - Network access
  - Libraries loaded by Win processes
  - Attempted access to privileged resources
- Docker:
  - Start/Stop services
  - Enable/disable ports

Galahad Use Case

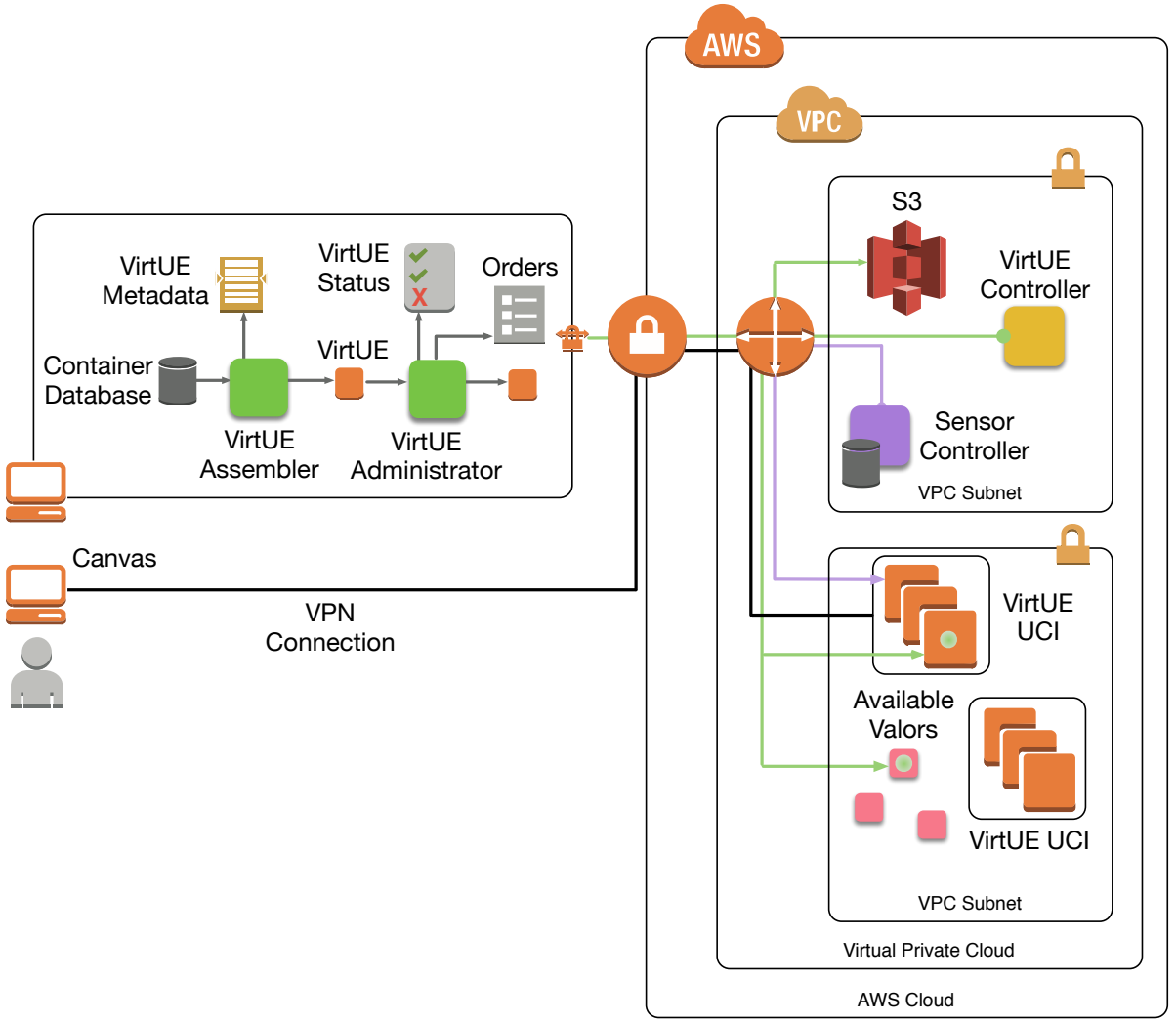


AWS Immutable Infrastructure

Galahad Components



Galahad Architecture



Questions?