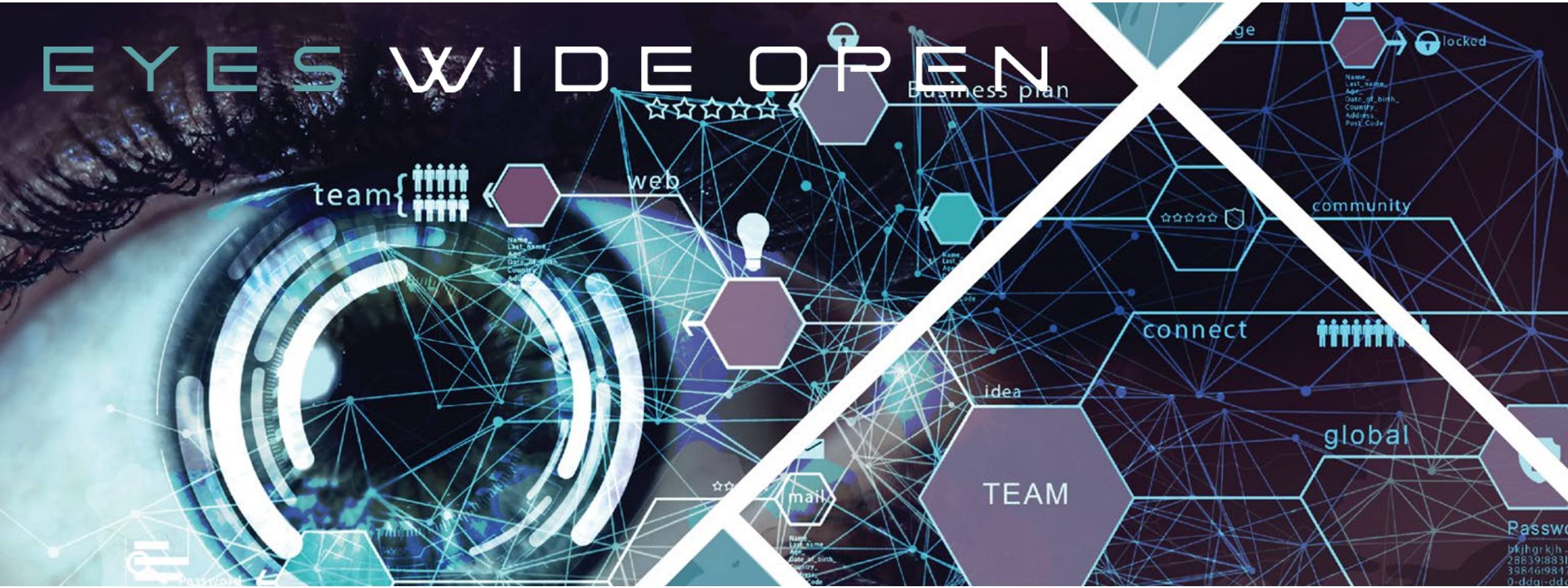
12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island



Monday Seminar

12:30 PM | Plaza 6

Technical Sessions

See page 18 in the Summit Guide for full details.

Panic Patching

Managing the Volume & Velocity of Alerts

Presented By:

Matt Ambroziak
Security Solutions Architect
Virsec

Christian Trujillo
Senior Solutions Architect
Red Hat

Session Overview

- Challenges with Vulnerabilities and Patching
- The Intention of Attackers
- Reduce Effort and Fatigue with Accuracy
- Technology to Avoid Panic Patching
- Elegantly Automate Patch Cycles

Vulnerabilities & Patches

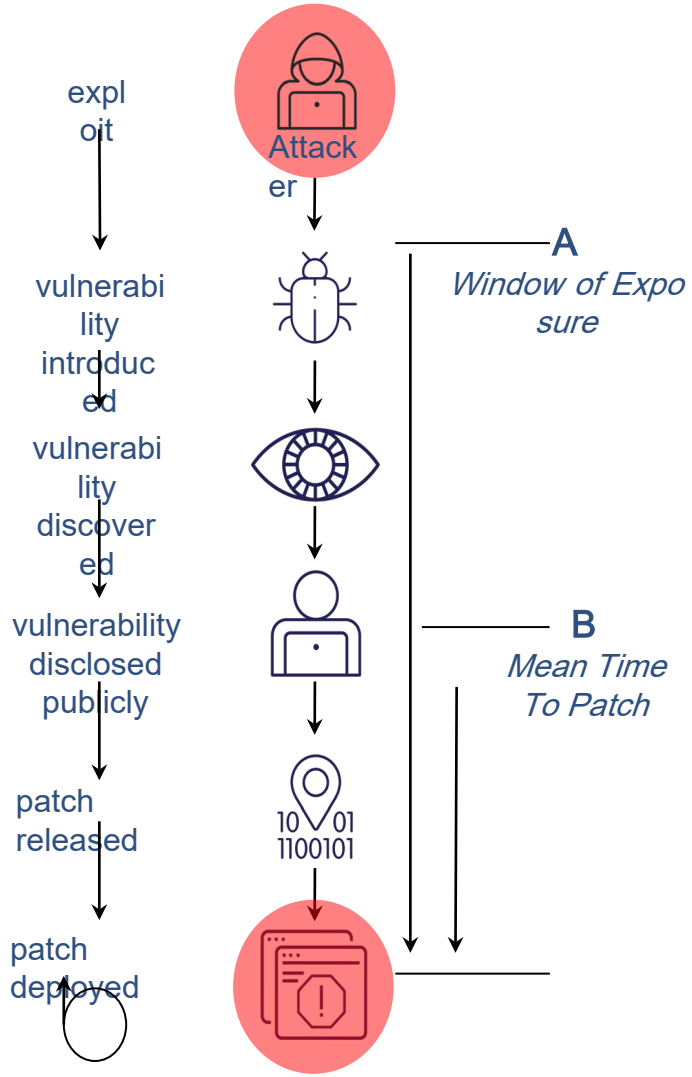
The Uphill Battle

Challenges for Patching in a Timely Manner

1. **Volume**
   Demand exceeds staffing, leaving known vulnerabilities unassigned
2. **Resources**
   Updating thousands of servers takes time and resources
3. **Critical Processes**
   Taking systems offline causes business disruption
4. **Policies**
   Many hoops to jump through to get the right patch to the right workload
5. **Legacy or Out-of-Support Applications**
   Commercial applications, no vendor support for packages or applications or the in-house development team is no longer available

The Zero-day Vulnerability Dilemma

Unpatched Vulnerabilities



What is it?

- Most tools compare patterns and signatures to known libraries of vulnerabilities.
- Zero-day vulnerabilities are **previously unknown** and do not have a repeating pattern.

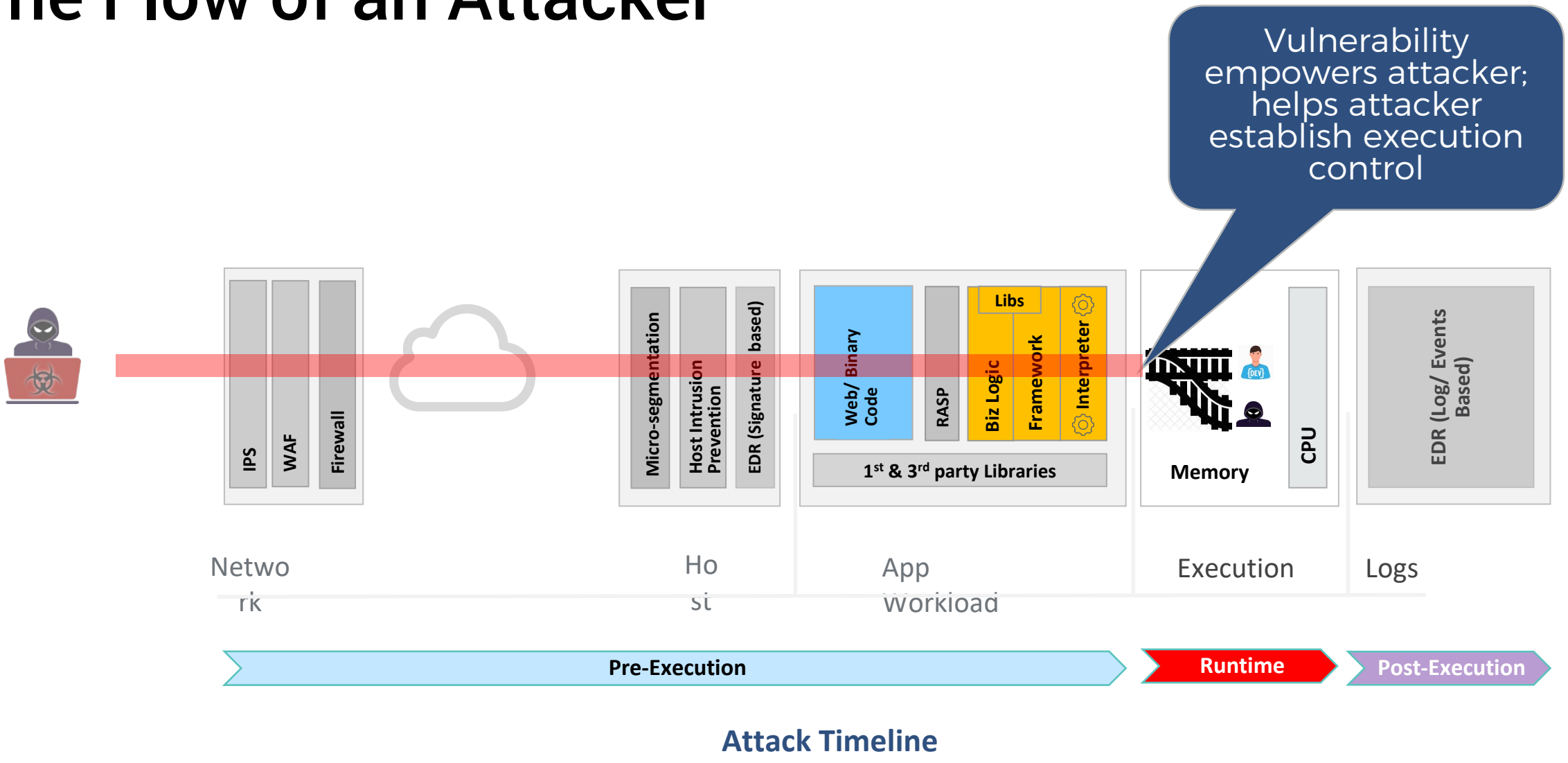
• Why is it so challenging?

- Protecting critical applications and infrastructure during the **dwell time** is challenging as no patch is available
- Overall, it took an average of **287 days to identify and contain** a data breach (IBM Security)
- Microsoft took **63 days to release a patch** for the Follina RCE vulnerability
- Average cost of a mega breach was **$401 million for a breaches** between 50 million and 65 million records

Server Workloads vs Attackers

"Servers do not wake up every day and do random things"

The Flow of an Attacker



Attack Timeline

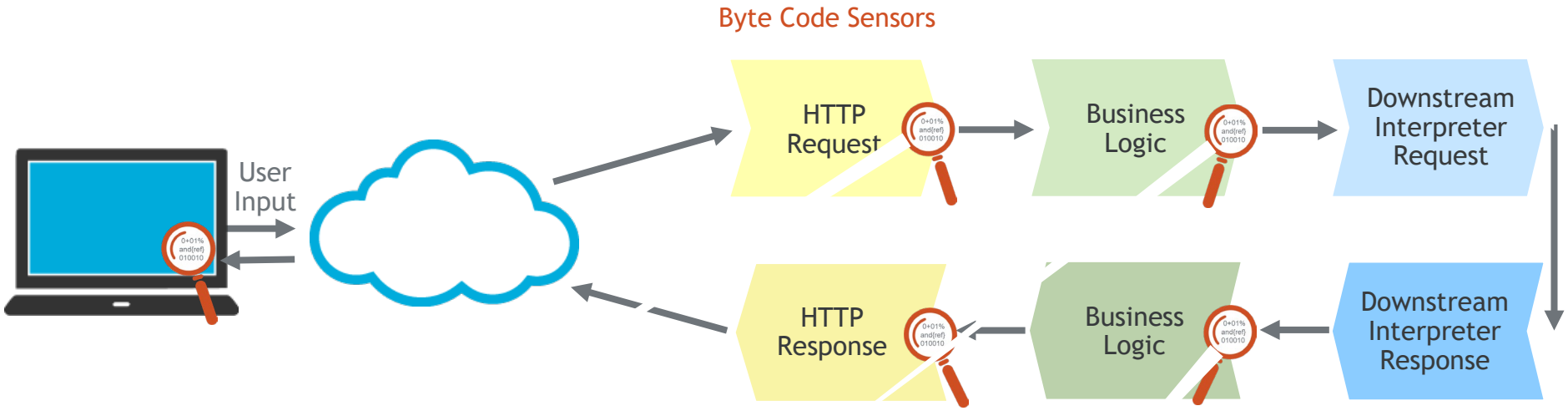
Block Exploits Upfront
→ Receive Alerts →
Trigger Patching Workflows

Continuous Workload Protection
& Automation Technologies
to Avoid Panic Patching

AVOID PANIC PATCHING
Protect Attacker Entry Points

Technologies to Protect Web Apps & Memory

Protecting Web Apps at Runtime



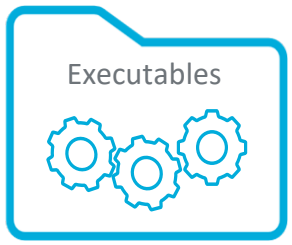
Web Attack Truth Table

Interpreter Syntax in HTTP Request	User Input in Interpreter Input	Interpreter Execution Status	Interpreter Syntax in HTTP Response	Benign/ Threat/ Attack
Yes	Yes	Success	Success	Attack
Yes	Yes	Fail	Fail	Threat
Yes	No	X	X	Benign

Select * from password_table where user = 'john' and password = 'xyz'

Select * from password_table where user = 'john' or 1 = 1 -- ~~and password = 'xyz'~~

Protecting App Memory at Runtime

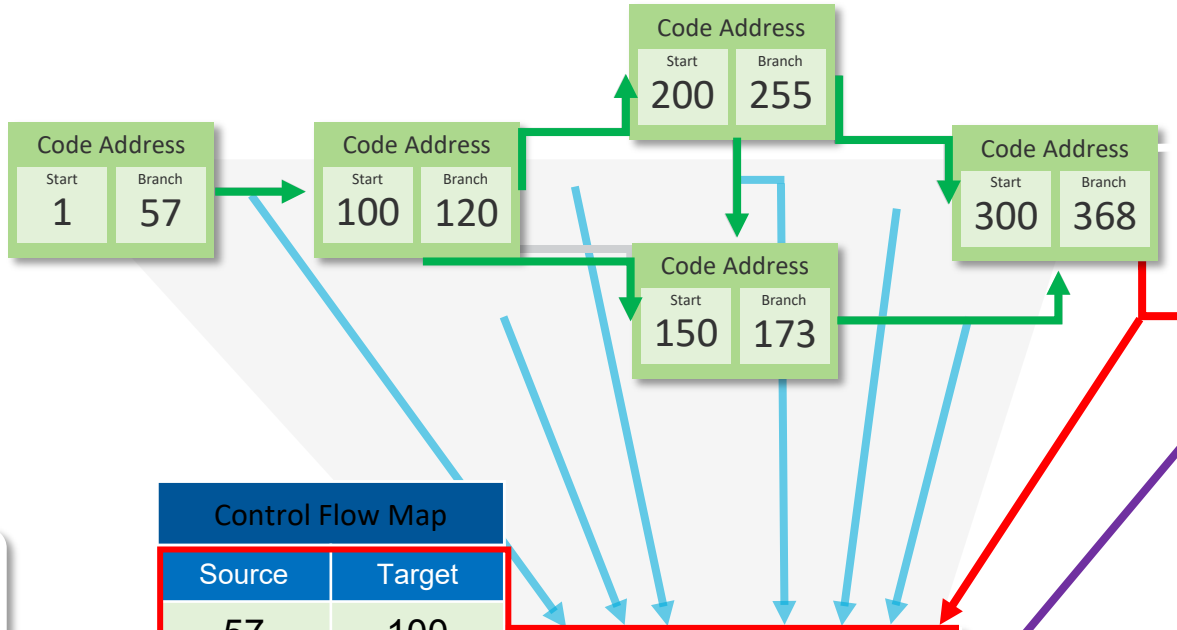


1 Verify File integrity before executing

2 Memory addresses assigned as code loads into memory

3 Control Flow map created without requiring source code

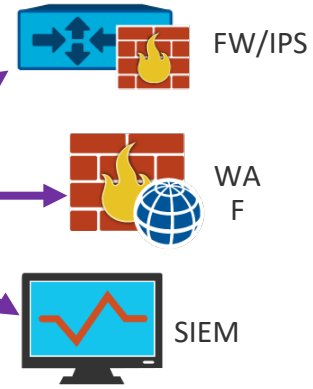
4 Monitor execution at every memory transition



Control Flow Map	
Source	Target
57	100
120	150
120	200
173	300
255	300
368	400
453	200

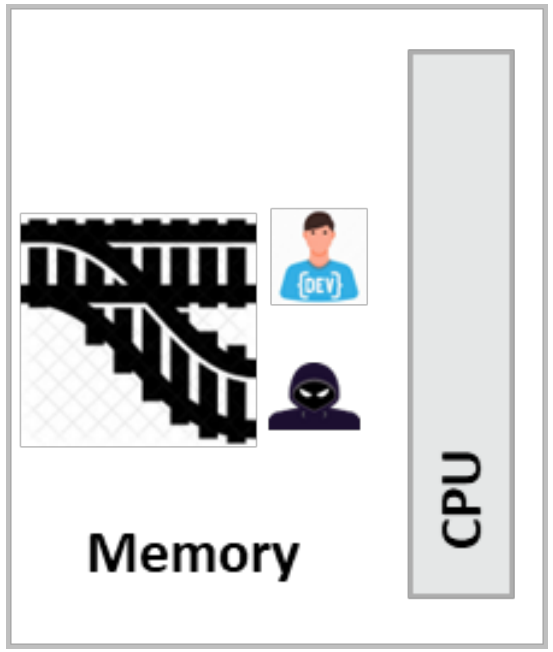
5 Malicious code causes an illegal “trampoline jump”

7 Micro protection actions can stop attack directly



8 Macro protection actions can disable access

Left Unprotected…
All Roads Lead to RCE



Protect Host Layer at Runtime

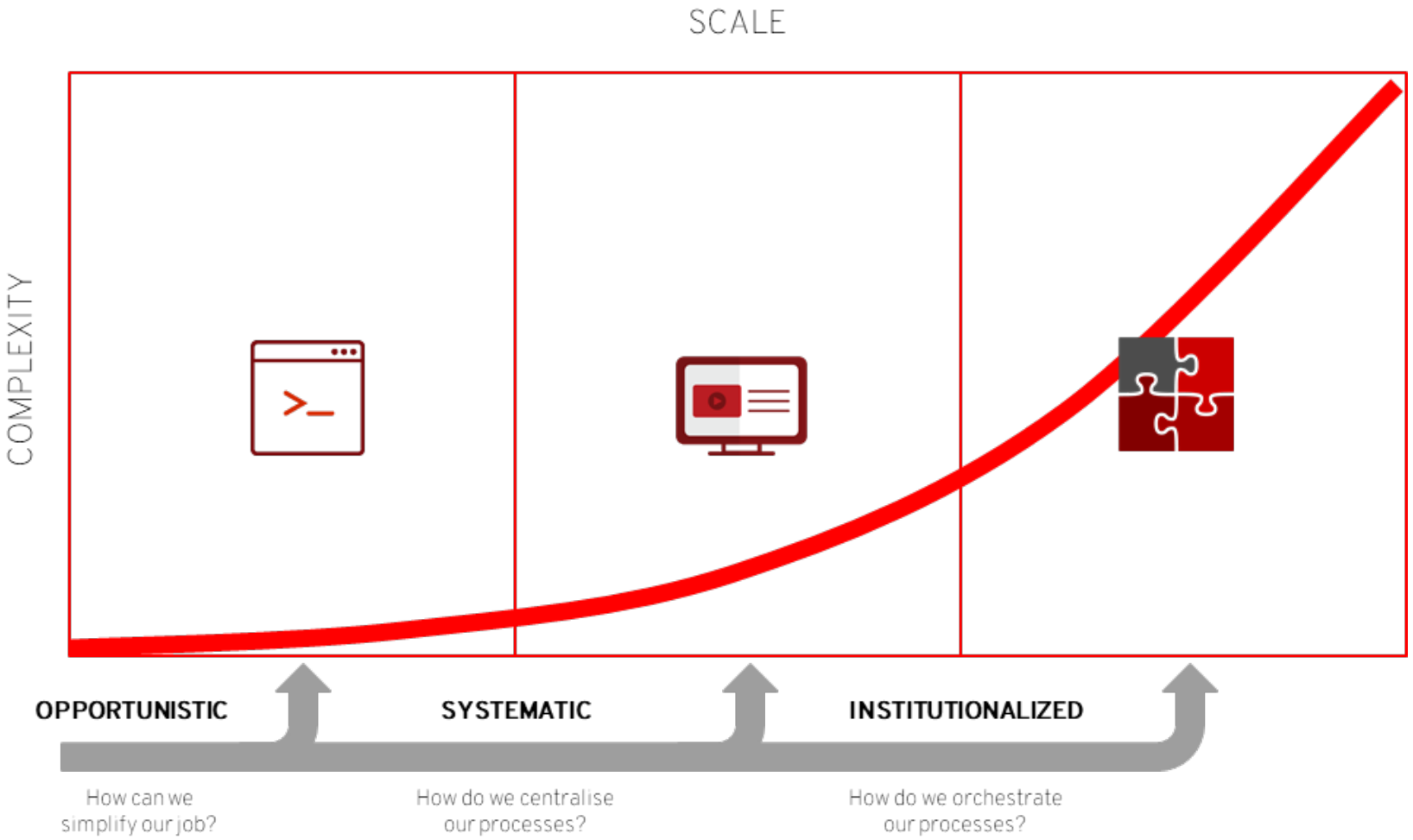
Application Control via Chains of Trusts and Allowlisting

- Executables
  - Decompose packages (RPM, MSI) and Extract Checksums
- Libraries
  - Decompose executables to find library dependencies
- Scripts
  - Establish allowed/disallowed combinations of Interpreter + Script

EYES WIDE OPEN
Accurate Alerts to Trigger Workflows

Automating Patch Workflows

Where are you in your Automation Journey?



Automation happens when one person meets a problem they never want to solve again

Teams are automating...

Lines Of Business

Network

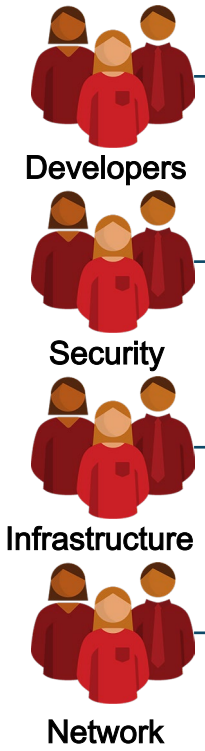
Security

Operations

Developers

Infrastructure

Ad-hoc Automation is happening in silos



Automation Platform used in silo

DIY scripting automation

Open source config management tool

Proprietary vendor supplied automation

Is organic automation enough?

Powerful Automation Tool

Simple

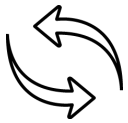
Human readable automation

No special coding skills needed

Tasks executed in order

Usable by every team

Get productive quickly



Powerful

App deployment

Configuration management

Workflow orchestration

Network automation

Orchestrate the app lifecycle

Agentless

Agentless architecture

Uses OpenSSH & WinRM

No agents to exploit or update

Get started immediately

More efficient & more secure

Automates technologies you use

Time to automate is measured in minutes

Cloud

AWS
Azure
Digital Ocean
Google
OpenStack
Rackspace
+more

Operating Systems

RHEL
Linux
Windows
+more

Virt & Container

Docker
VMware
RHV
OpenStack
OpenShift
+more

Storage

Netapp
Red Hat
Storage
Infinidat
+more

Windows

ACLs
Files
Packages
IIS
Regedits
Shares
Services
Configs
Users
Domains
+more

Network

A10
Arista
Aruba
Cumulus
Bigswitch
Cisco
Dell
Extreme
F5
Lenovo
MikroTik
Juniper
OpenSwitch
+more

Security

Checkpoint
Cisco
CyberArk
F5
Fortinet
Juniper
IBM
Palo Alto
Snort
+more

Monitoring

Dynatrace
Datadog
LogicMonitor
New Relic
Sensu
+more

Devops

Jira
GitHub
Vagrant
Jenkins
Slack
+more

What Can I Automate ?

Automate the deployment and management of your entire IT footprint.

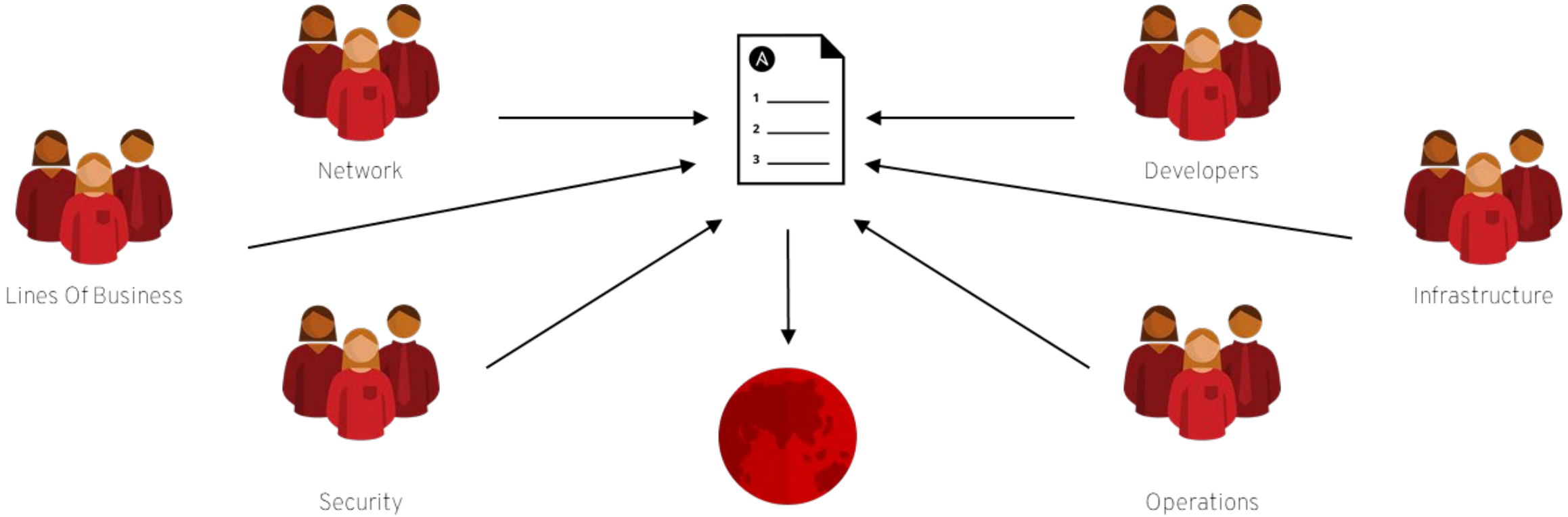
Do this...

- Orchestration
- Configuration Management
- Application Deployment
- Provisioning
- Continuous Delivery
- Security and Compliance

On these...

- Firewalls
- Load Balancers
- Applications
- Containers
- Clouds
- Servers
- Infrastructure
- Storage
- Network Devices
- **And more...**

When automation crosses teams, you need an automation platform



Strategic Use Cases

Automating The Security Ecosystem

Security Information & Events Management

splunk>

IBM

Enterprise Firewalls

Check Point SOFTWARE TECHNOLOGIES LTD

CISCO

f5

FORTINET

JUNIPER NETWORKS

Workload Protection Platforms

virsec

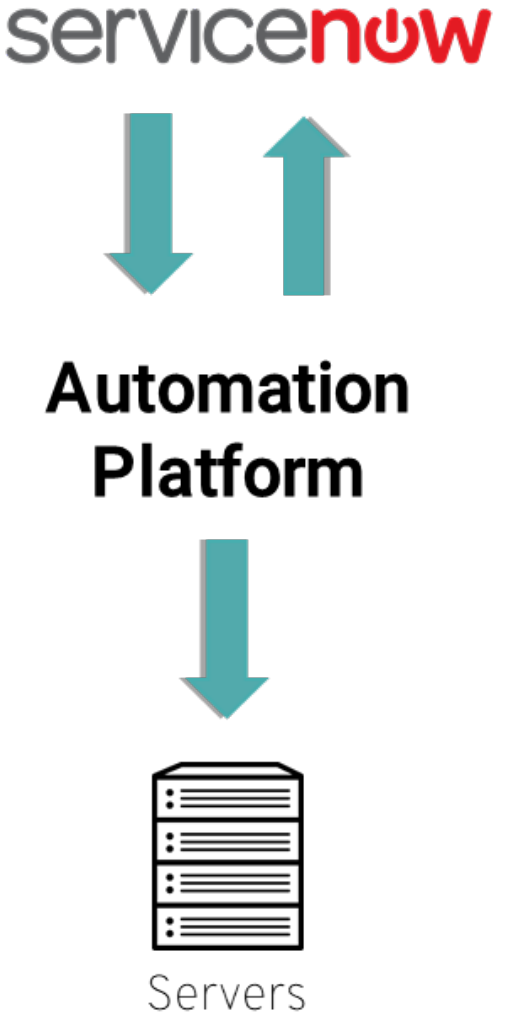
Privileged Access Management

CYBERARK

Syncope

WORKFLOW AUTOMATION

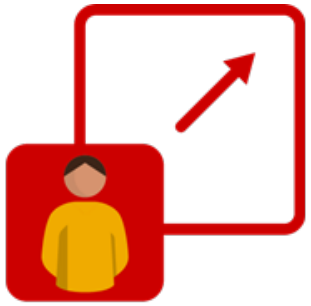
- Great customer support starts at your ITSM
- Automation broker
- Close the ticketing loop



How Automation solves today's security operations challenges

Speed

Reduce the number of manual steps and GUI-clicking, enable the orchestration of security tools and accelerate their interaction with each other



Reduce Human Errors

Minimize risks with automated workflows, avoid human operator errors in time-sensitive, stressful situations

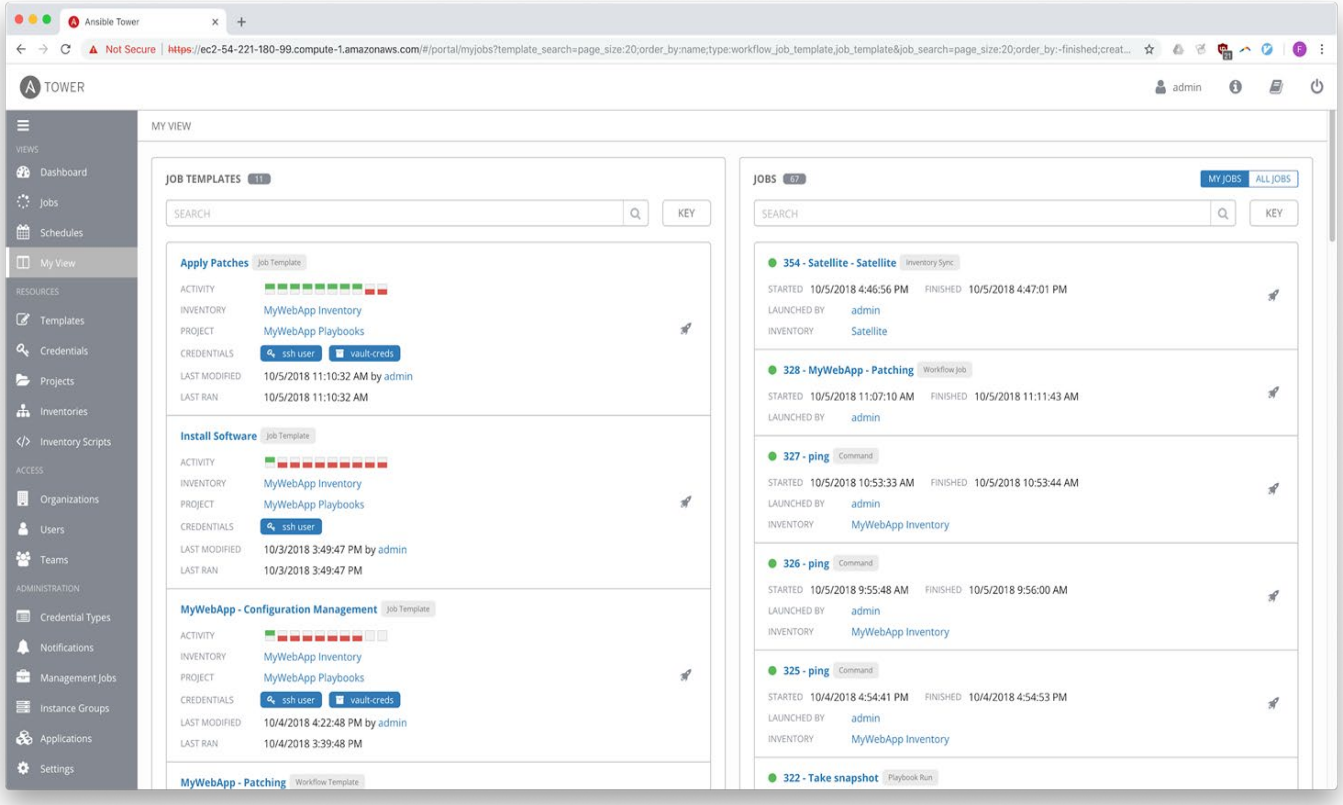
Consistency

Enable auditable and verifiable security processes by using a single tool and common language covering multiple security tools

PATCHING

MORE THAN PUSHING PACKAGES

- Where's the pain?
  - Maintenance windows and downtime
  - Security exposure
  - Point tools - Satellite, WSUS, SCCM
- Automates the ENTIRE patching process
    - Start/stop application/database services
    - Snapshots
    - Remove system(s) from LB pool
    - Patch more than the OS
- Unifies point tools and leverages their best features

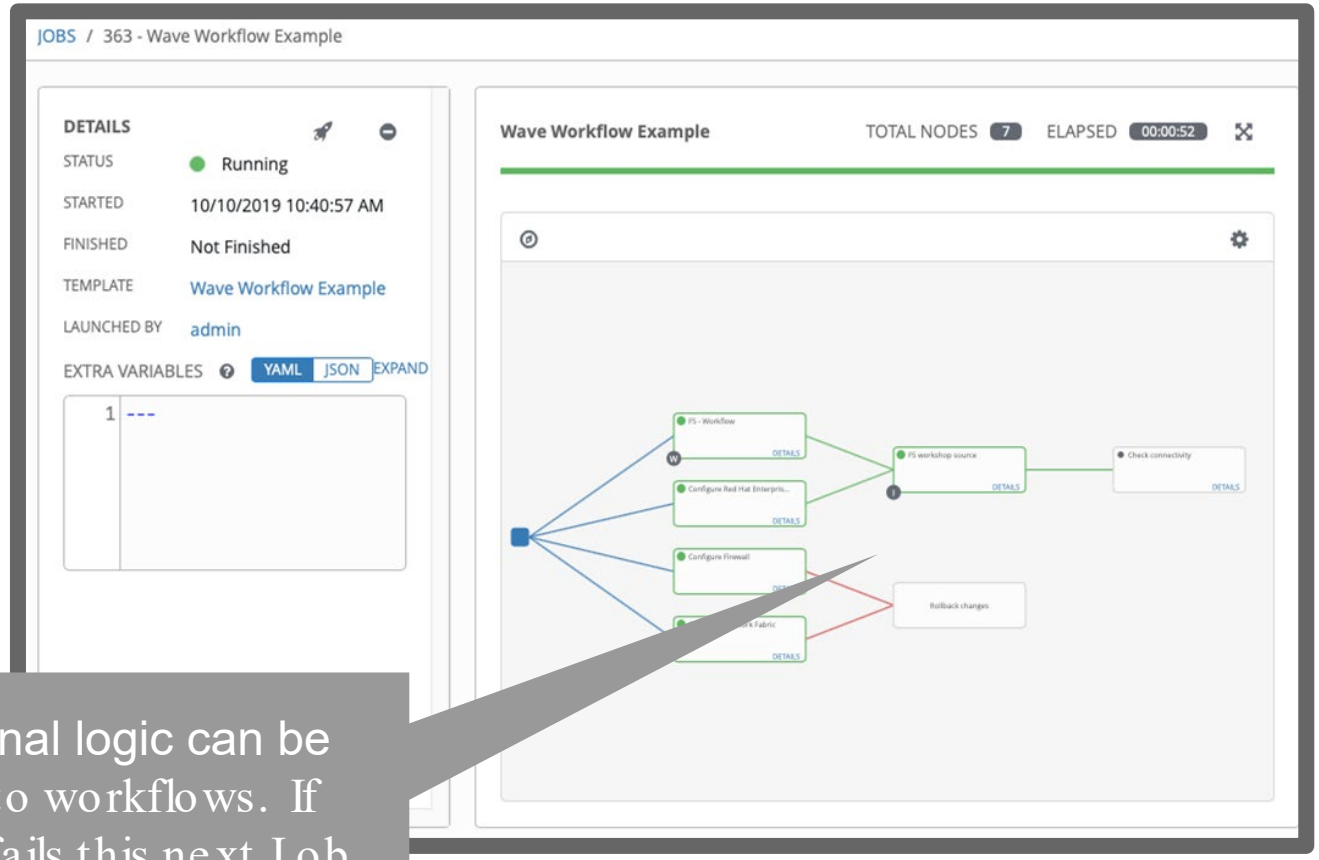


Workflows

Create powerful holistic automation using Ansible Workflows.

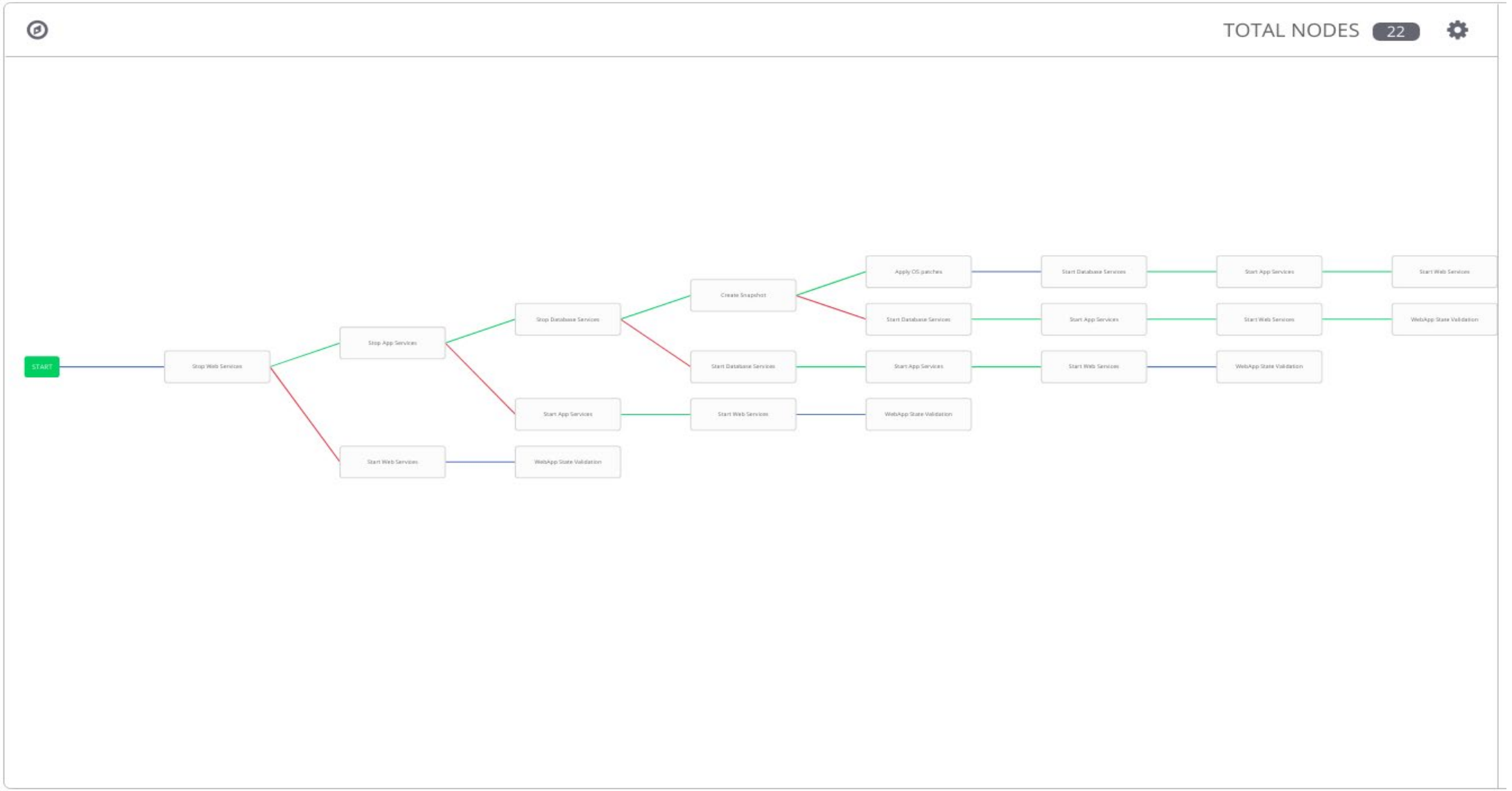
Orchestration can easily be configured by linking Job Templates.

Workflow approvals allow Workflows to pause and wait for human interaction

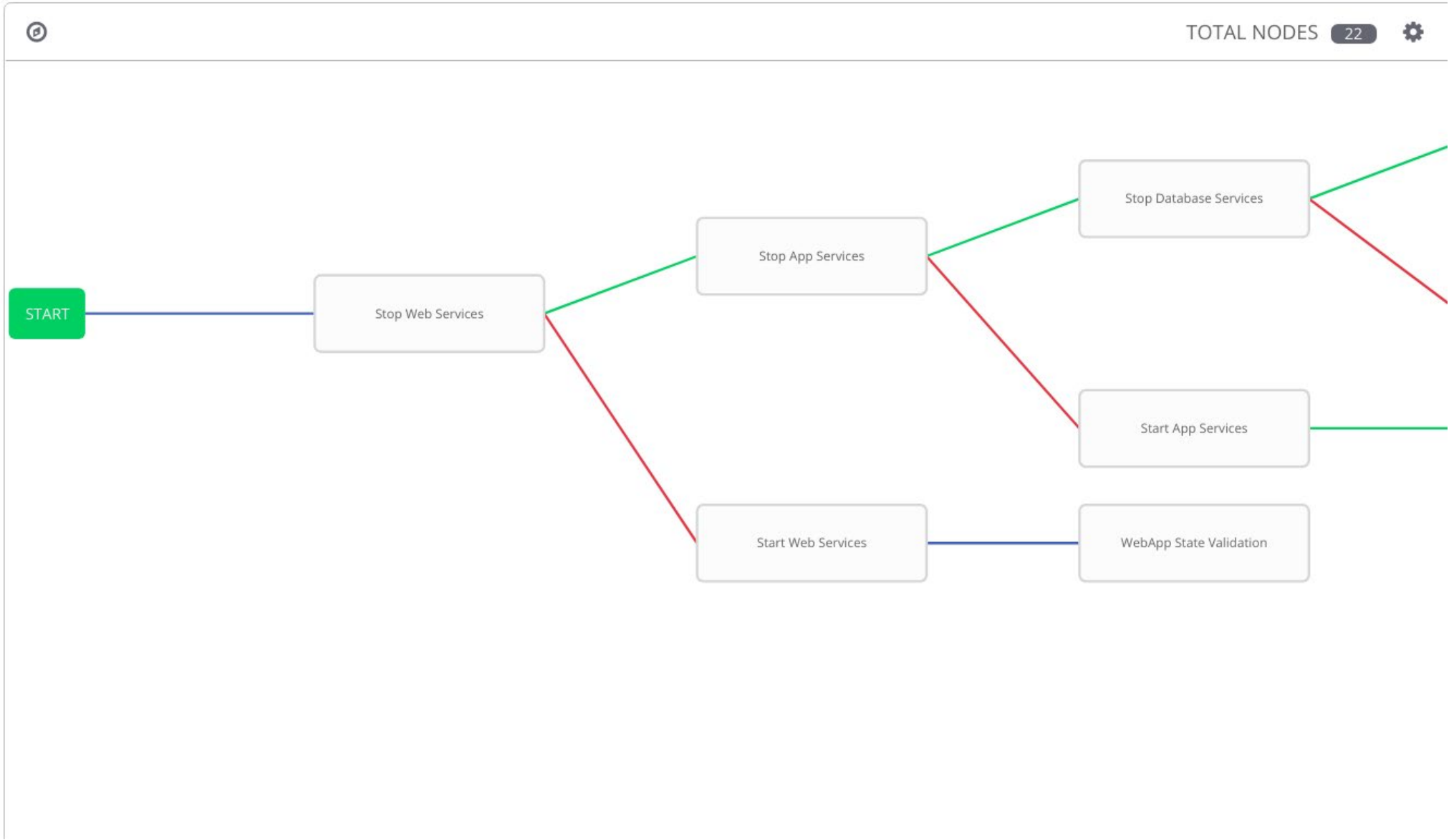


Conditional logic can be applied to workflows. If this job fails this next Job is run!

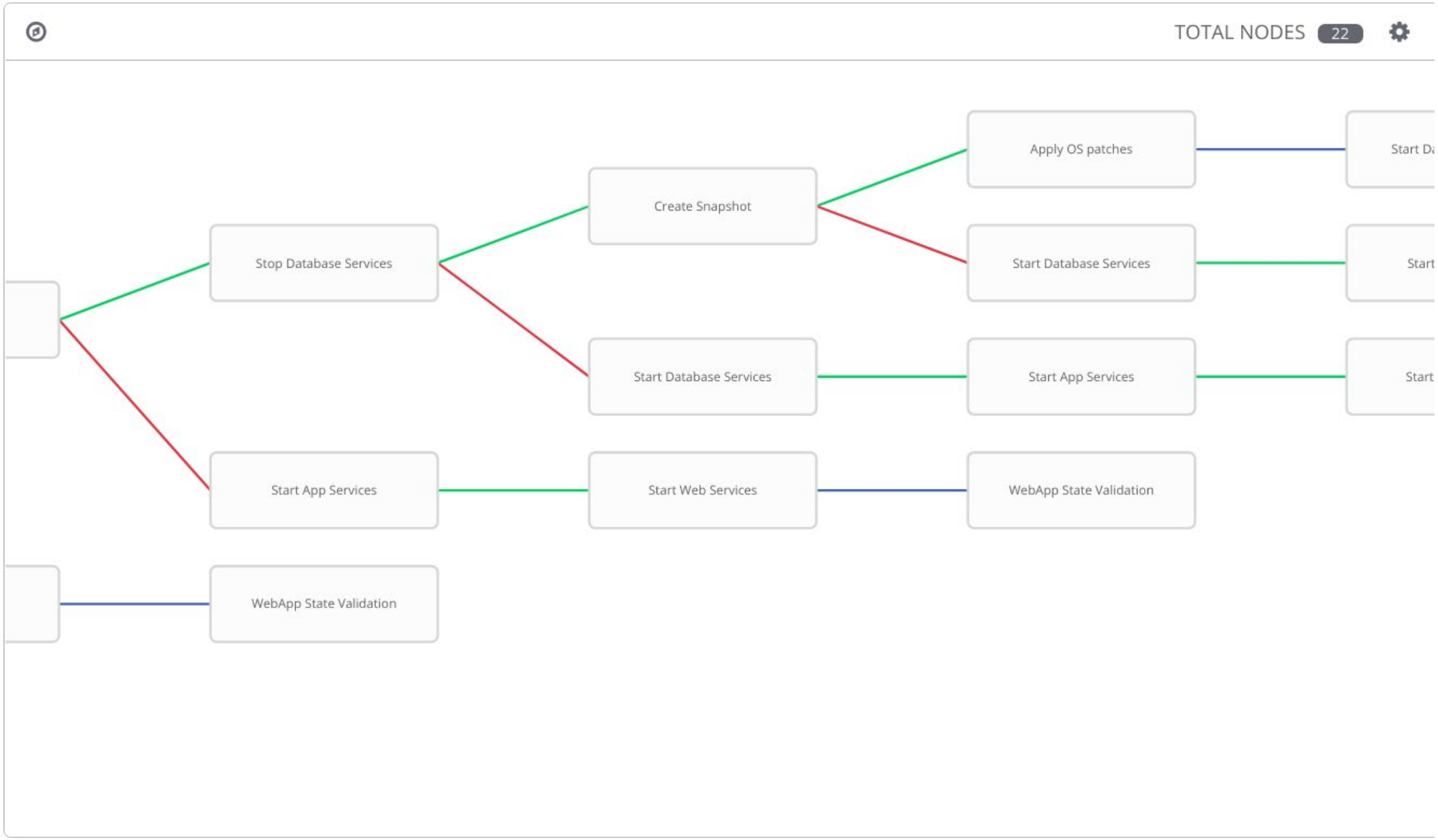
WORKFLOW VISUALIZER | WebApp OS Maintenance



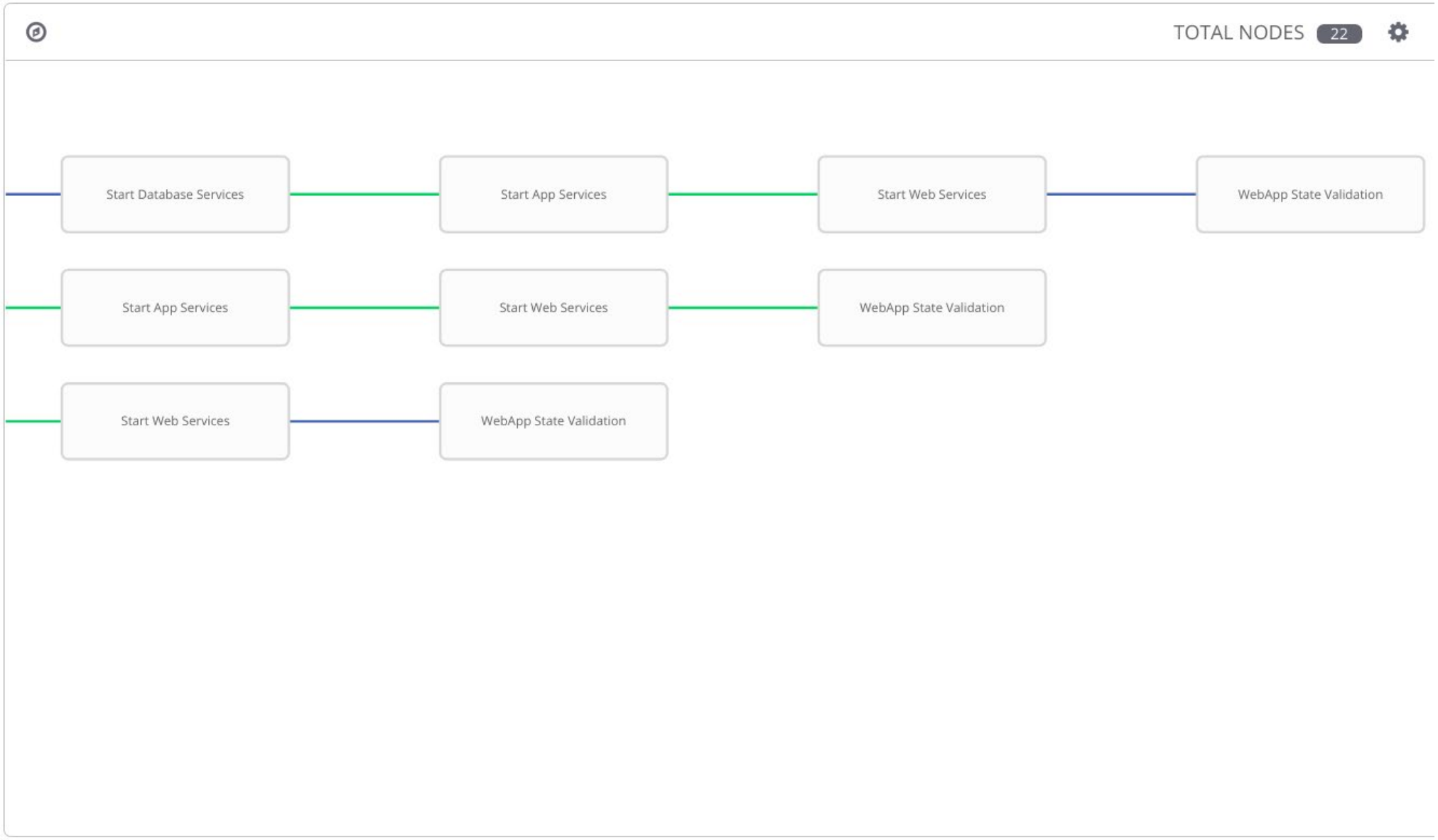
WORKFLOW VISUALIZER | WebApp OS Maintenance



WORKFLOW VISUALIZER | WebApp OS Maintenance



WORKFLOW VISUALIZER | WebApp OS Maintenance



Questions

Virsec and Red Hat

Better Together in Automating Server Workload Protection

Visit us in the Expo Hall @ Booth #404

virsec™

Red Hat

Thank You