



Security

Christopher Martin

<http://ChristopherMartin.WORK>

# Risk Management

## Define Risk Analysis – Quantitative vs Qualitative

### Identify Application / Data risk exposure factor

Which applications, data impose more financial risk within the organization.  
Is the asset exposed?

What is the monetary loss for one particular event?

Are multiple breaches expected in a given year?

What's the Return on Investment / Total cost of Ownership for spending  
budget on security?

### Risk Assessment to the business

Invest in security where it makes sense for the business. For example, an application that is not exposing critical data may not justify the spend for security vs another app with more exposure.

An application with more ports, network connectivity to it is higher justification for security. .

# Enterprise Governance System

## Management Objectives

Align, Plan,  
Organize

Build, Acquire,  
Implement

Deliver,  
Service,  
Support

Monitor,  
Evaluate<  
Assess

| Risk | Importance | Performance | <b>Importance</b> = How important it is for the organization on a scale from 1 (not at all) to 5 (very)<br><b>Performance</b> = How well it is done from 1 (very well) to 5 (do not know or badly)<br><b>Formality</b> = Existence of a contract, an SLA or a clearly documented procedure (Yes, No or ?)<br><b>Audited</b> = Yes, No or ?<br><b>Accountable</b> = Name or 'do not know'<br><b>Domains and Objectives</b> | Who does it? |       |         |             |         |           | Who is accountable? |
|------|------------|-------------|---|--------------|-------|---------|-------------|---------|-----------|---------------------|
|      |            |             |   | IT           | Other | Outside | Do Not Know | Audited | Formality |                     |
|      |            |             | Governance  |              |       |         |             |         |           |                     |
|      |            |             | Evaluate, Direct and Monitor  |              |       |         |             |         |           |                     |
|      |            |             | EDM01 Ensured Governance Framework Setting and Maintenance  |              |       |         |             |         |           |                     |
|      |            |             | EDM02 Ensured Benefits Delivery   |              |       |         |             |         |           |                     |
|      |            |             | EDM03 Ensured Risk Optimization   |              |       |         |             |         |           |                     |
|      |            |             | EDM04 Ensured Resource Optimization   |              |       |         |             |         |           |                     |
|      |            |             | EDM05 Ensured Stakeholder Engagement  |              |       |         |             |         |           |                     |
|      |            |             | Management  |              |       |         |             |         |           |                     |
|      |            |             | Align, Plan and Organize  |              |       |         |             |         |           |                     |
|      |            |             | APO01 Managed I&T Management Framework  |              |       |         |             |         |           |                     |
|      |            |             | APO02 Managed Strategy  |              |       |         |             |         |           |                     |
|      |            |             | APO03 Managed Enterprise Architecture   |              |       |         |             |         |           |                     |
|      |            |             | APO04 Managed Innovation  |              |       |         |             |         |           |                     |
|      |            |             | APO05 Managed Portfolio   |              |       |         |             |         |           |                     |
|      |            |             | APO06 Managed Budget and Costs  |              |       |         |             |         |           |                     |
|      |            |             | APO07 Managed Human Resources   |              |       |         |             |         |           |                     |
|      |            |             | APO08 Managed Relationships   |              |       |         |             |         |           |                     |
|      |            |             | APO09 Managed Service Agreements  |              |       |         |             |         |           |                     |
|      |            |             | APO10 Managed Vendors   |              |       |         |             |         |           |                     |
|      |            |             | APO11 Managed Quality   |              |       |         |             |         |           |                     |
|      |            |             | APO12 Managed Risk  |              |       |         |             |         |           |                     |
|      |            |             | APO13 Manage Security   |              |       |         |             |         |           |                     |
|      |            |             | APO14 Managed Data  |              |       |         |             |         |           |                     |
|      |            |             | Build, Acquire and Operate  |              |       |         |             |         |           |                     |
|      |            |             | BAI01 Managed Programs  |              |       |         |             |         |           |                     |
|      |            |             | BAI02 Managed Requirements Definition   |              |       |         |             |         |           |                     |
|      |            |             | BAI03 Managed Solutions Identification and Build  |              |       |         |             |         |           |                     |
|      |            |             | BAI04 Managed Availability and Capacity   |              |       |         |             |         |           |                     |
|      |            |             | BAI05 Managed Organizational Change   |              |       |         |             |         |           |                     |
|      |            |             | BAI06 Managed IT Changes  |              |       |         |             |         |           |                     |
|      |            |             | BAI07 Managed IT Change Acceptance and Transitioning  |              |       |         |             |         |           |                     |
|      |            |             | BAI08 Managed Knowledge   |              |       |         |             |         |           |                     |
|      |            |             | BAI09 Managed Assets  |              |       |         |             |         |           |                     |
|      |            |             | BAI10 Managed Configuration   |              |       |         |             |         |           |                     |
|      |            |             | BAI11 Managed Projects  |              |       |         |             |         |           |                     |
|      |            |             | Deliver, Service and Support  |              |       |         |             |         |           |                     |
|      |            |             | DSS01 Managed Operations  |              |       |         |             |         |           |                     |
|      |            |             | DSS02 Managed Service Requests and Incidents  |              |       |         |             |         |           |                     |
|      |            |             | DSS03 Managed Problems  |              |       |         |             |         |           |                     |
|      |            |             | DSS04 Managed Continuity  |              |       |         |             |         |           |                     |
|      |            |             | DSS05 Managed Security Services   |              |       |         |             |         |           |                     |
|      |            |             | DSS06 Managed Business Process Controls   |              |       |         |             |         |           |                     |
|      |            |             | Monitor, Evaluate and Assess  |              |       |         |             |         |           |                     |
|      |            |             | MEA01 Managed Performance and Conformance Monitoring  |              |       |         |             |         |           |                     |
|      |            |             | MEA02 Managed System of Internal Control  |              |       |         |             |         |           |                     |
|      |            |             | MEA03 Managed Compliance with External Requirements   |              |       |         |             |         |           |                     |
|      |            |             | MEA04 Managed Assurance   |              |       |         |             |         |           |                     |

# Implement Framework

Steps to safeguard against threats / Risk

Use internal resources, software to establish a baseline of ongoing normal metrics.

Standardized process for image revisions, patches, config changes review, and implementation.

Determine external connectivity through LAN, WIFI for vulnerabilities.

Analyze shared information with third parties, including but not limited to supply chain, managed services.

Review policies that govern resources access and information sharing.

Inventory systems, evaluate hardening, configuration.

Evaluate human behavior, usage.

Security training, awareness.



# Business Continuity Planning

## Define customer Continuity Metrics

Customer defined recovery metrics for private / commercial cloud:

Maximum Tolerable Downtime:

Recovery Point / Time Objective:

Mean time to failure /; repair:



# Compliance / Incident Response

Internal resources responsible for security policy, standards, management and response

Assigned roles, responsibilities within customer to analyze log input, regularly practice incident response, recovery.

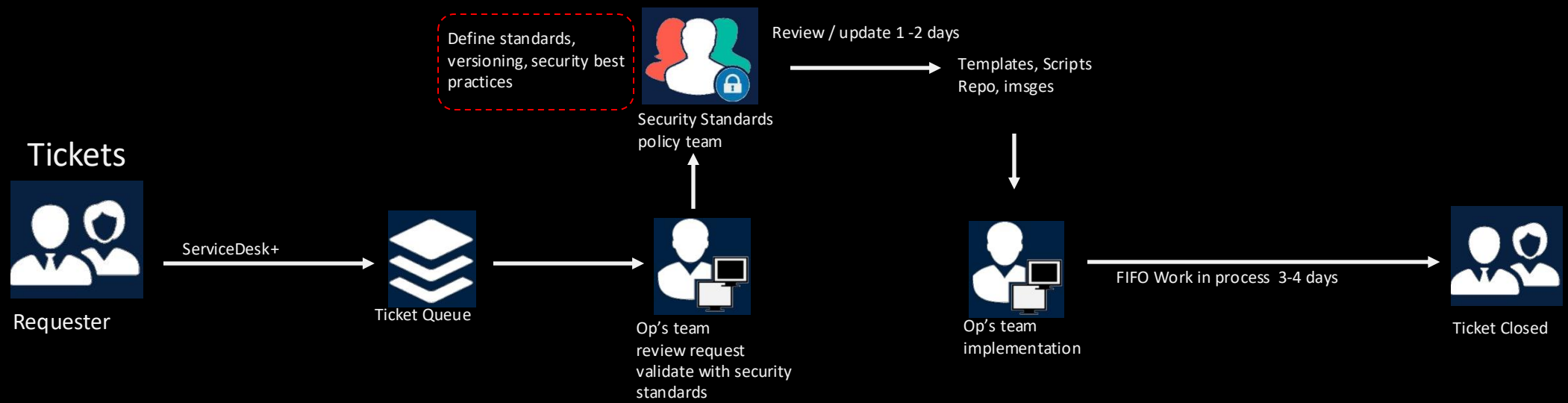
Define company policy for image, config, deployment standards.

Imbed the Incident response framework into the organization.

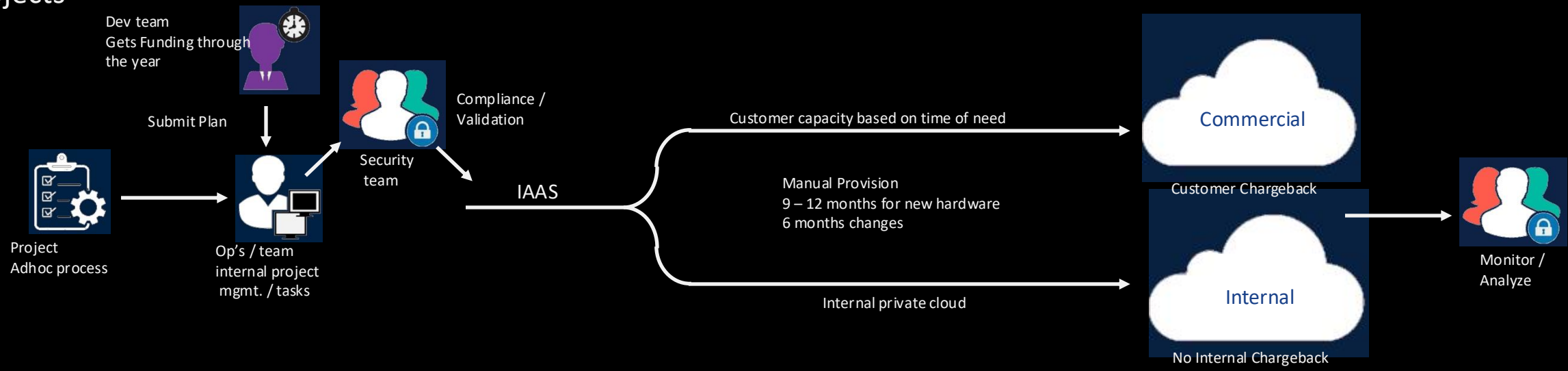
Perform Chaos Engineering tasks to test the vulnerability of systems and processes.

# Customer Security Recommendations

# Customer Security Compliance Process



## Projects

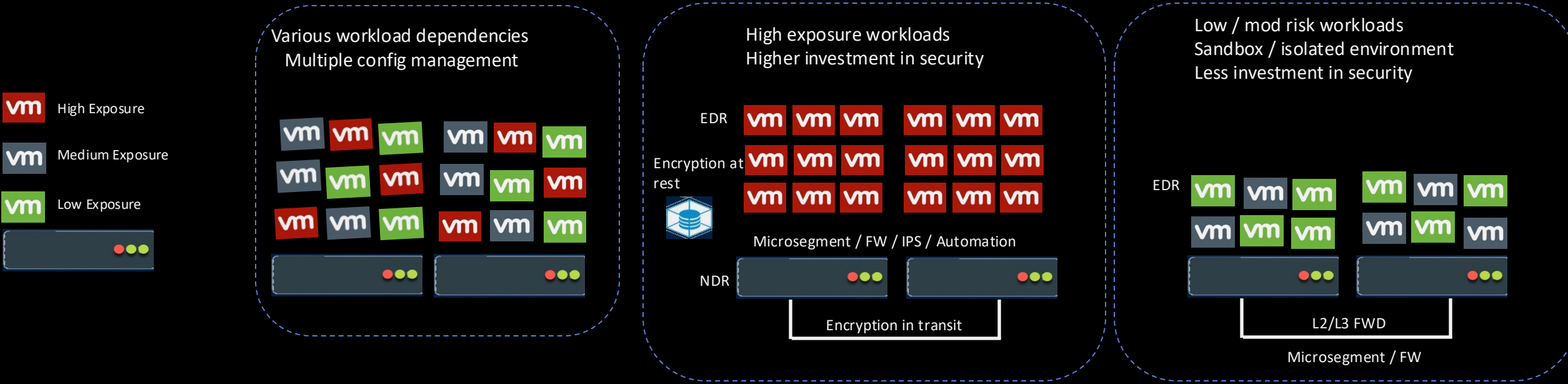


# Application Exposure Risk

Categorize Applications, workloads based on dependency, exposure level to Customer.

Invest in security, policies based on the exposure level to the business.

Microsegment and encrypt data in transit and at rest where appropriate.

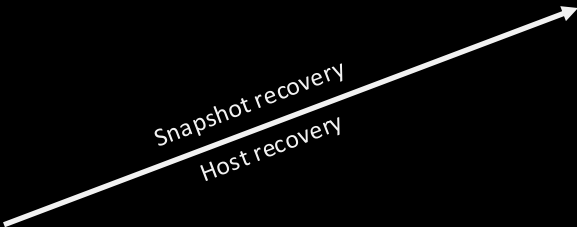
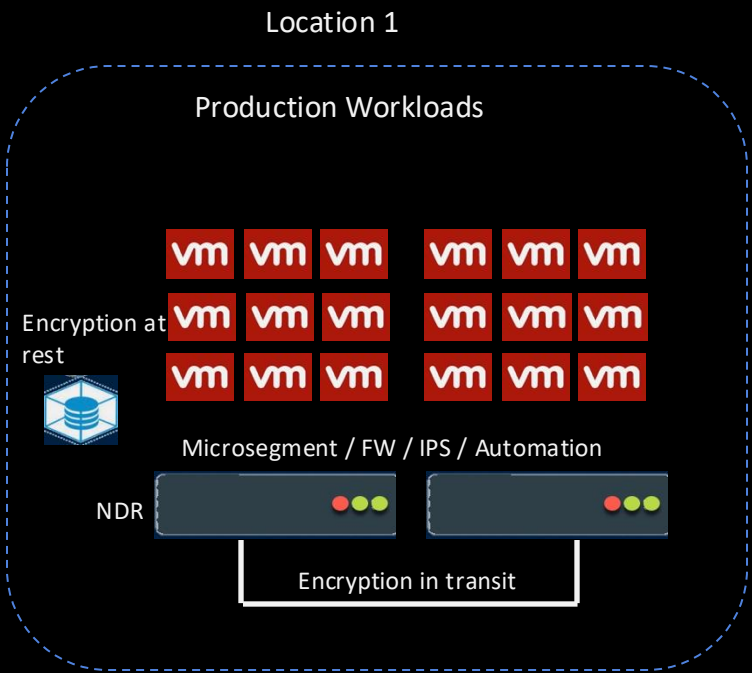


# Business Continuity

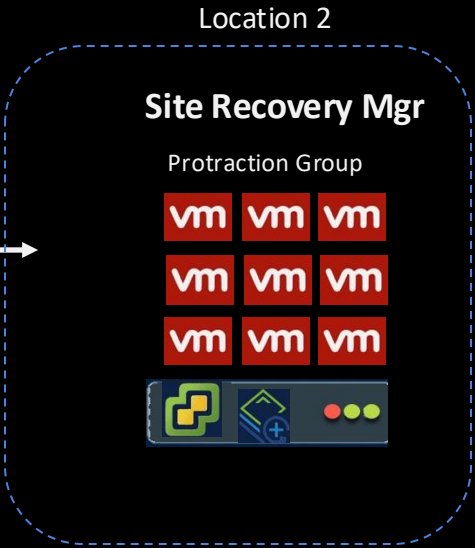
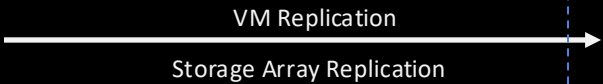
Categorize Applications, workloads based on dependency, exposure level to Customer.

Invest in security, policies based on the exposure level to the business.

Microsegment and encrypt data in transit and at rest where appropriate.



| Failover / Fallback |               |                    |
|---------------------|---------------|--------------------|
| Type                | VCDR          | SRM                |
| RPO                 | 4 hours       | Low RPO            |
| RTO                 | On-demand     | Fast pre provision |
| REP                 | Cloud Storage | VMC                |

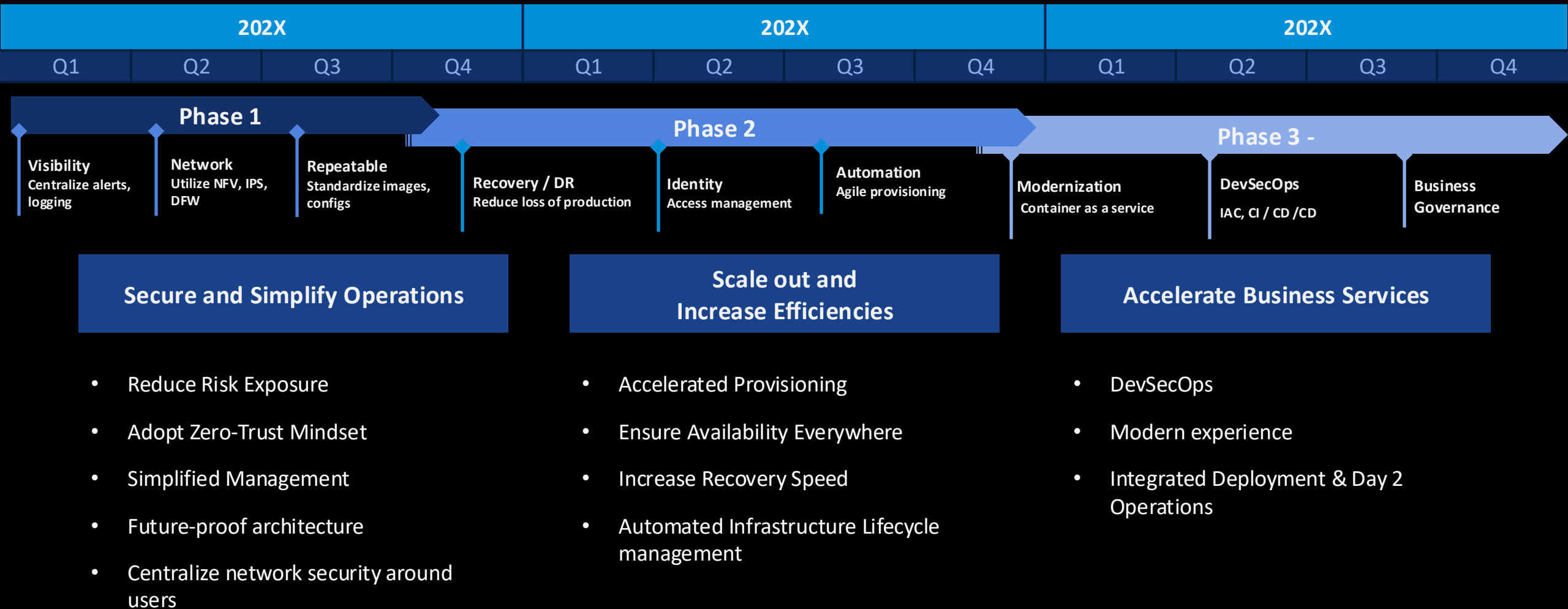


| Failover / Fallback |                            |
|---------------------|----------------------------|
| Type                | SRM                        |
| RPO                 | Synchronous<br>5 min RPO   |
| RTO                 | Fast RTO with<br>Many VM's |
| REP                 | Vcenter at<br>MAUSICA      |

# Customer Phased Future State

# Value Realization timeline

Capability and Value Combine to Create Business Impact



# Phase I Secure and Simplify Operations

Initiatives to build a secure future state architecture

## Visibility

Security, incident response teams to consolidate logging, alerting metrics to a central repository for analysis, ongoing monitoring.

## NFV

Extend L3 boundary to the virtualization layer, policy and inspect application traffic for E/W, N/S patterns.

## Imaging

Standardize image repositories, versioning, patch remediation prior for production workloads.

## Provisioning

Define and deploy templates, scripts for standardized provisioning of workloads based on exposure level.

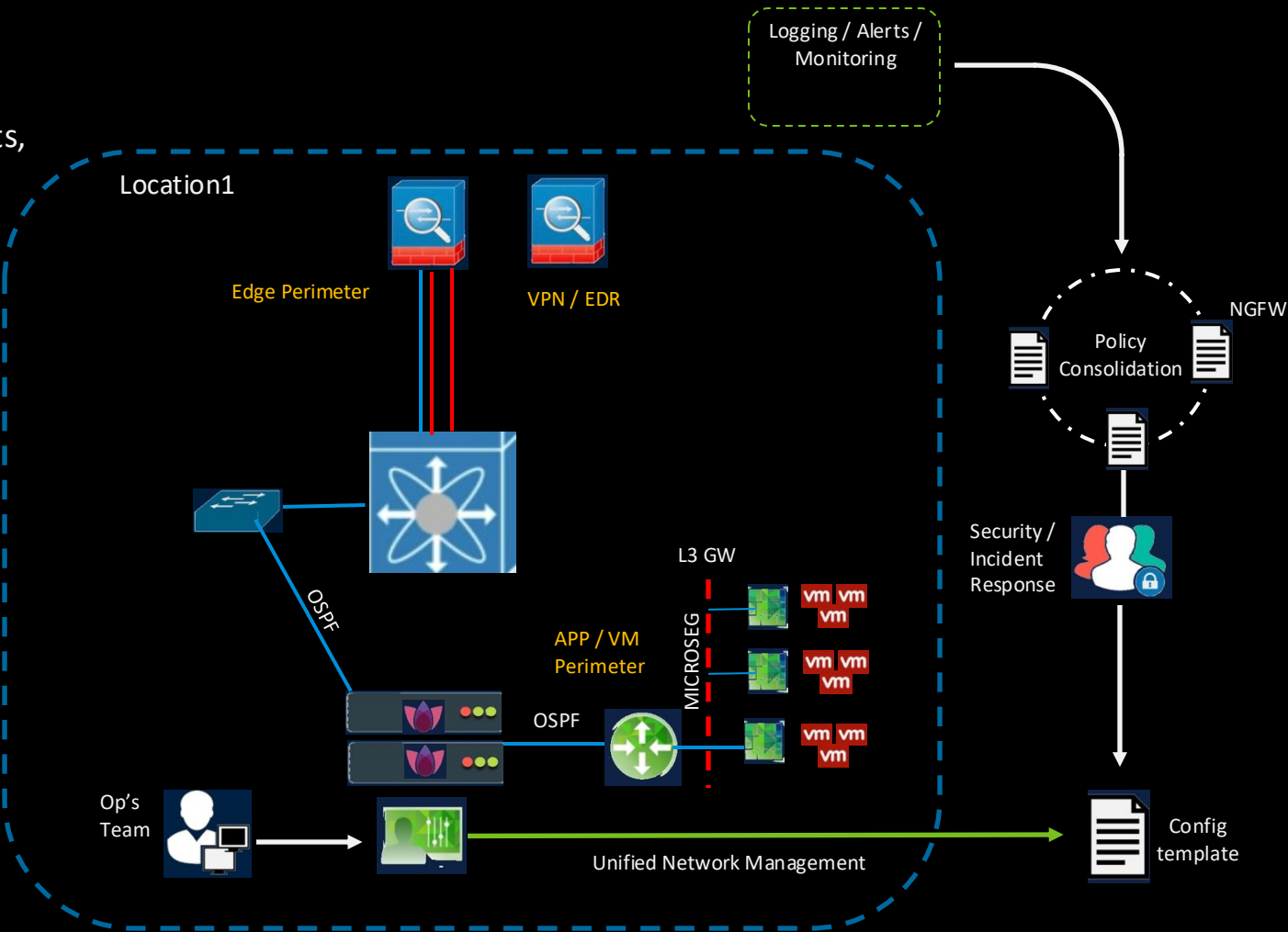


# Extend NFV Services

Enable software-based routing, security policies for applications for E/W and outbound traffic flows.

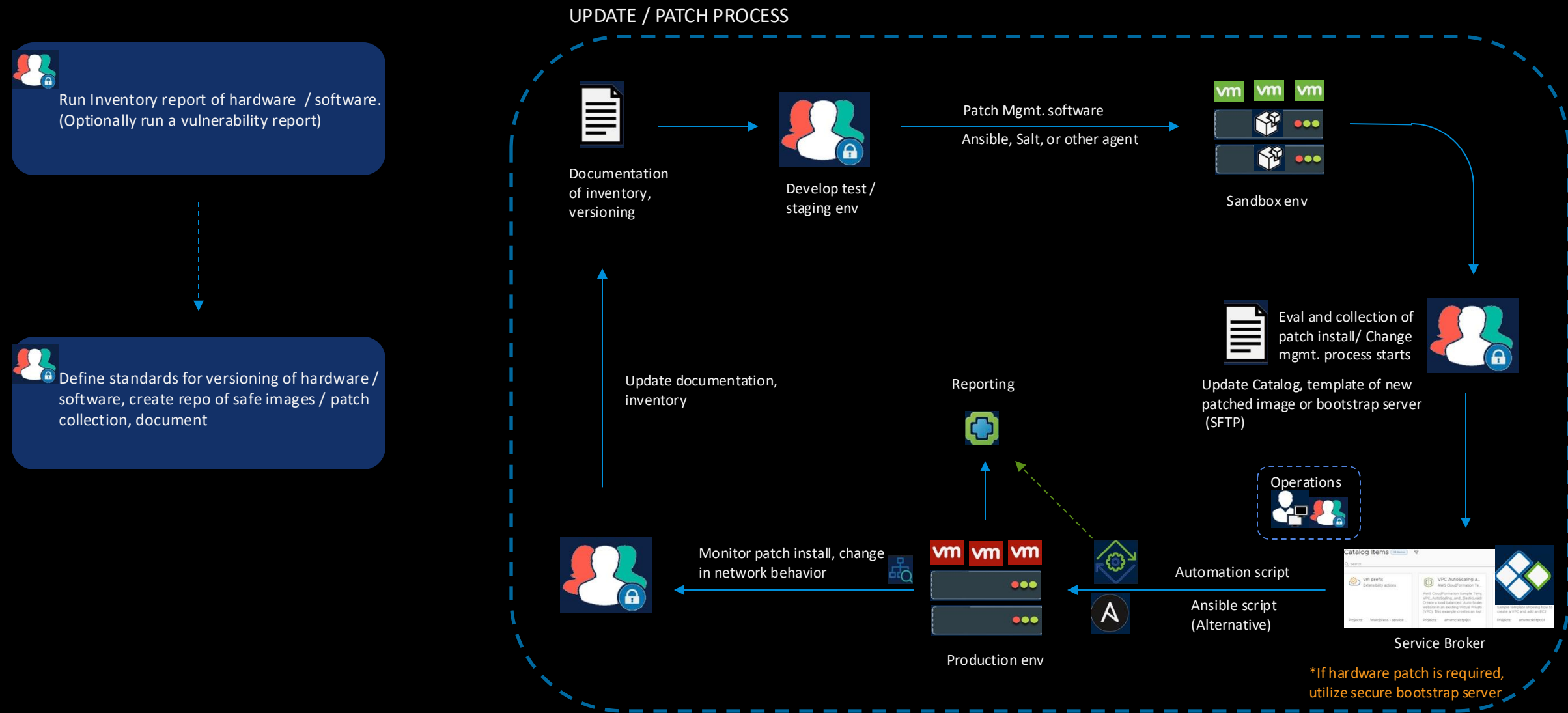
Separate security boundaries allows for consolidation Of rulesets, for troubleshooting and management.

Config templates continually checked for compliance with NetFlow, logging reports



# Image / Patch Management and Provisioning

Process for continuous patching hardware and software.



# Workload Protection

## Safeguarding data inside VM's

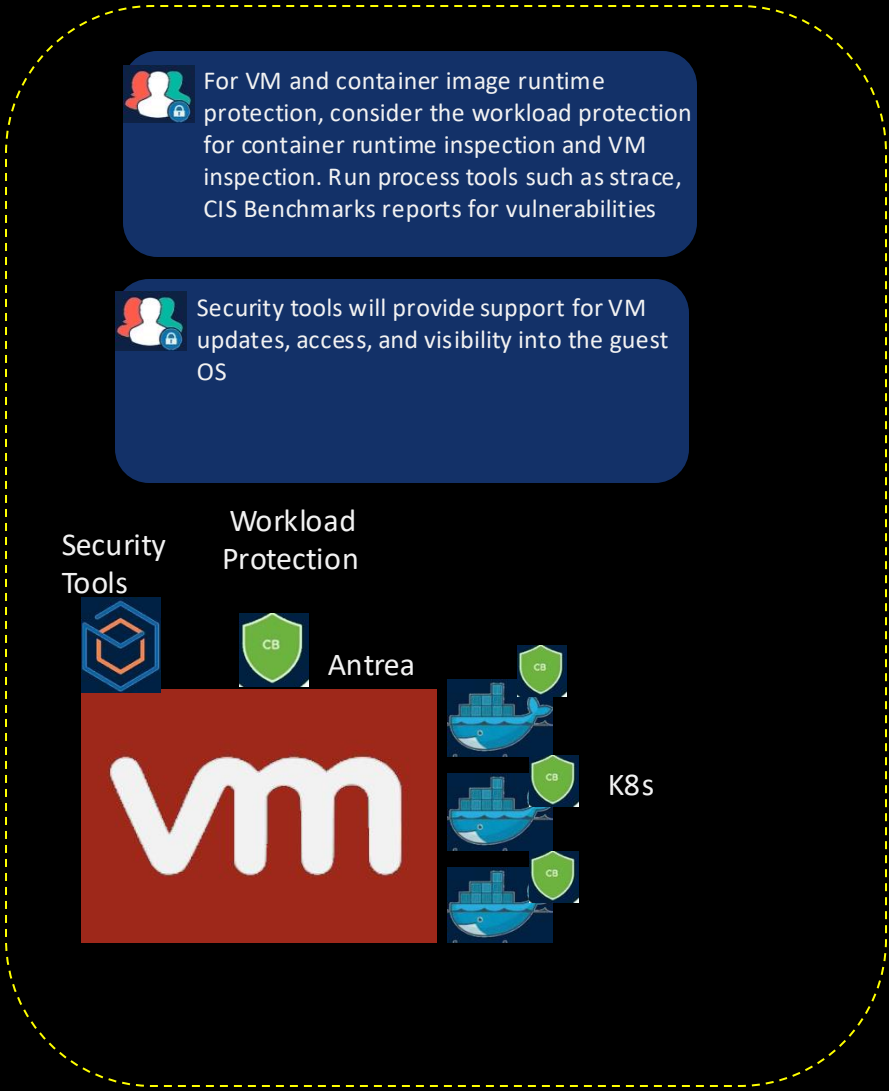
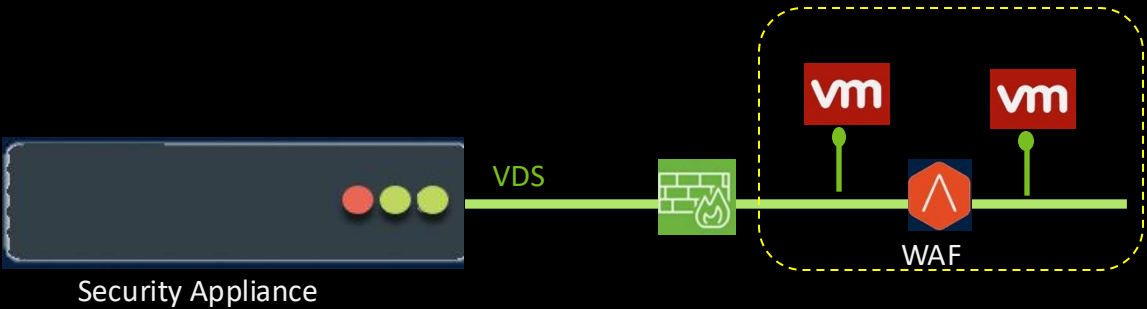
- IPS ATP scans for malicious content within the networking traffic to the Vm based on signature-based DB of known attacks
- WAF is aware of the user accessing the web app, session information to the application vs signatures

- Validate the security software can view inside the VM and container runtime inspection for injection attacks, cross scripting

- WAF will provide IP intelligence, proactive BOT defense, credential protection, etc

- For VM and container image runtime protection, consider the workload protection for container runtime inspection and VM inspection. Run process tools such as strace, CIS Benchmarks reports for vulnerabilities

- Security tools will provide support for VM updates, access, and visibility into the guest OS



# Phase I Summary

Run a vulnerability report, implement and consolidate logs, monitoring to a specific team within Customer account.

Upgrade to FW for E/W traffic policy enforcement and routing. Utilize IPS for inspection of traffic, consolidate rulesets for specific function.

Incorporate a patch mgmt. process with automation to reduce provisioning times but also provides ease of deployment and management



# Phase II Scale Out and Increase Efficiencies

Meet business demands while reducing provisioning times and risk.

## Scale out

Decouple hardware dependencies from software configurations  
with automation to scale workloads


## Identity Access

Identification, Authentication, Authorization and Accounting


## Recovery

Enable fast RTO / RPO for quick recovery of images, VM's exposed to vulnerability.


# Identity Access with Existing Architecture



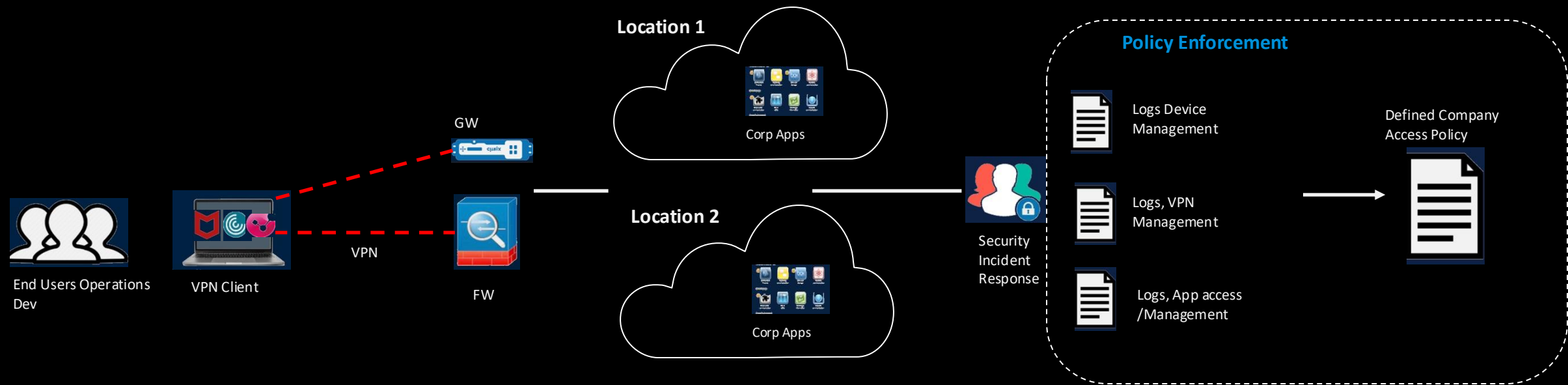
EDR, NDR log alerting from different vendor toolsets to be centrally collected for review



Align policy configurations with each solution to compliment access retractions for onboarding, or removal of employee access



Integrate LDAP / Radius (if possible) with each security solution to control user access at the domain level.



# Phase II Summary

Phase II to be completed after Phase I initiatives

LDAP / Radius integration for Server cluster, network access, administration

Centralize remote user access through an on-prem authentication server.  
Consider VDI, Agent / Agentless access methods for more strict control on user access and MFA.

Implement DR between Location1 and Location 2, after exposure risk assessment has been complete, and workloads are micro segmented, and categorized.

# Phase III App Modernization / Future Services

Modernize applications to internally to accelerate services and grow business revenue from customer service offerings

## DevSecOps

Evaluate and update code dependencies and potential vulnerabilities. Utilize toolsets to help with automating workflows for secure container images.

## Modernize Application LCM

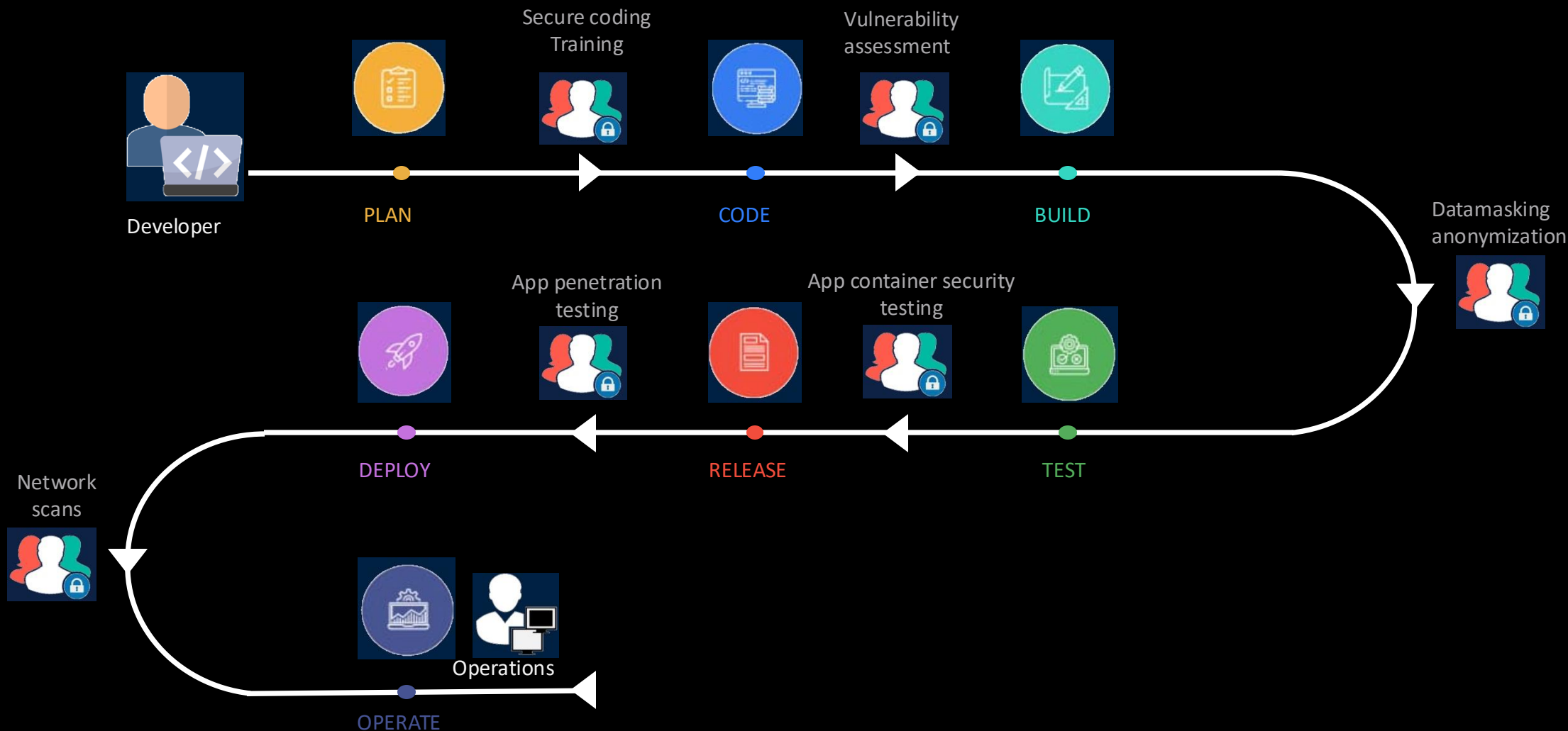
Integrate Kubernetes with container runtime and infrastructure for management and visibility for both Dev and Ops.

## Day 2 Operations

Universal control plane using Software Toolsets for CI / CD / CD workflows and automated tasks.

# Development Process

DevOps key checkpoints for security



# Implementing DevSecOps

