Enabling Zero Trust all the way to the edge

DAFITC 2025

Department of the Air Force Information Technology & Cyberpower (DAFITC):
A Training and Education Event

Chad Hobbs

Associate Principal Specialist Solution Architect - Red Hat

About Me

Associate Principal Specialist Solution Architect - Ansible

Why should you listen to me?

- Navy Veteran - Served on the USS Ronald Reagan
- Part of Navy Manpower migration from MS Access to SAP
- Helped build WPAFB 445th Airlift Wing IT infrastructure
- Developed novel application security app for the VA's VBMS
- Designed and built SEC IA plan for largest financial DB in the world
- Defined container security strategy for DHA Operations
- Participate in Red Hat's Zero Trust Special Interest Group

Today’s Agenda

Defining the Threat
Containers and Immutability
Restricted and Disconnected
Security through Policy Enforcement
Scaling Zero Trust with Automation

The Threat Landscape

Tactical Risk Scenarios

Why Traditional Perimeter Security Fails

Defining The Threat

We have been living in an evolving threat landscape.

- Nation-state cyber actors within IT systems
- Supply chain compromises at all levels
- Expanding electronic warfare capabilities, both hot and cold

A chain reaction: inside the cyberattack that brought vendor to its knees

By Ed Williams published 22 July 2025

Cyberattack exposes fragility of interconnected supply chains

10 GW satellite killer? Country designs microwave weapon to fry spacecraft in orbit

Military draws inspiration from Cold War-era Soviet science to design an ultra-powerful microwave weapon.

Updated: Aug 01, 2025 07:41 AM EST

Warning MoD weapons test could scramble GPS

16 June 2025

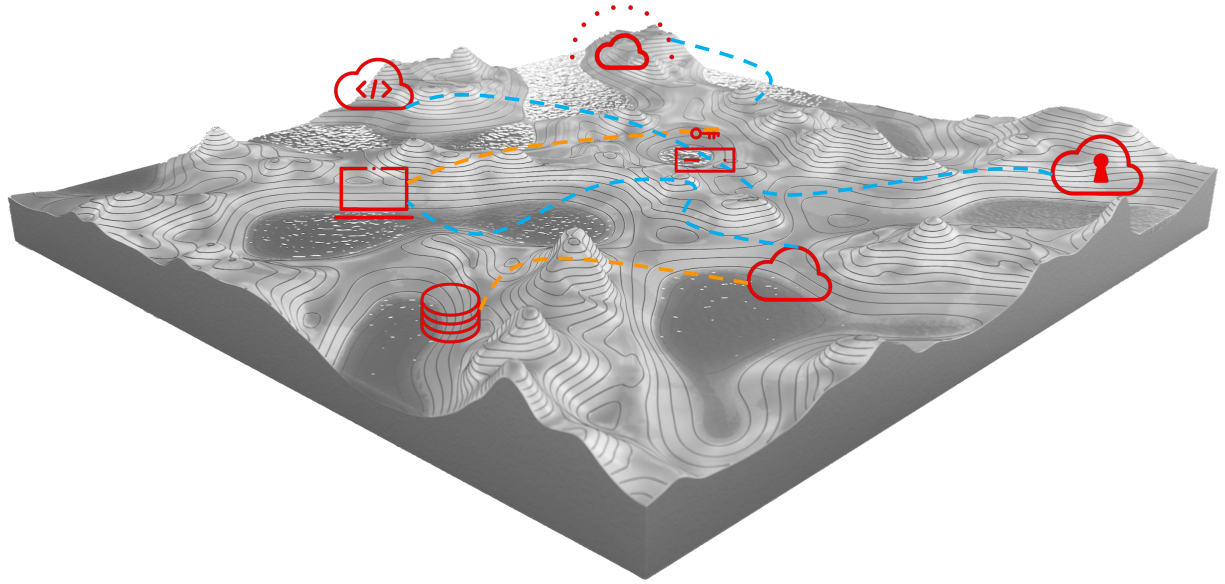
Country's new electronic warfare tech disrupts enemy systems while protecting friendly signals

The innovation is based on two drones acting in conjunction. They cancel each other out at the point of intersection, creating a 'null zone' for ally communication to operate.

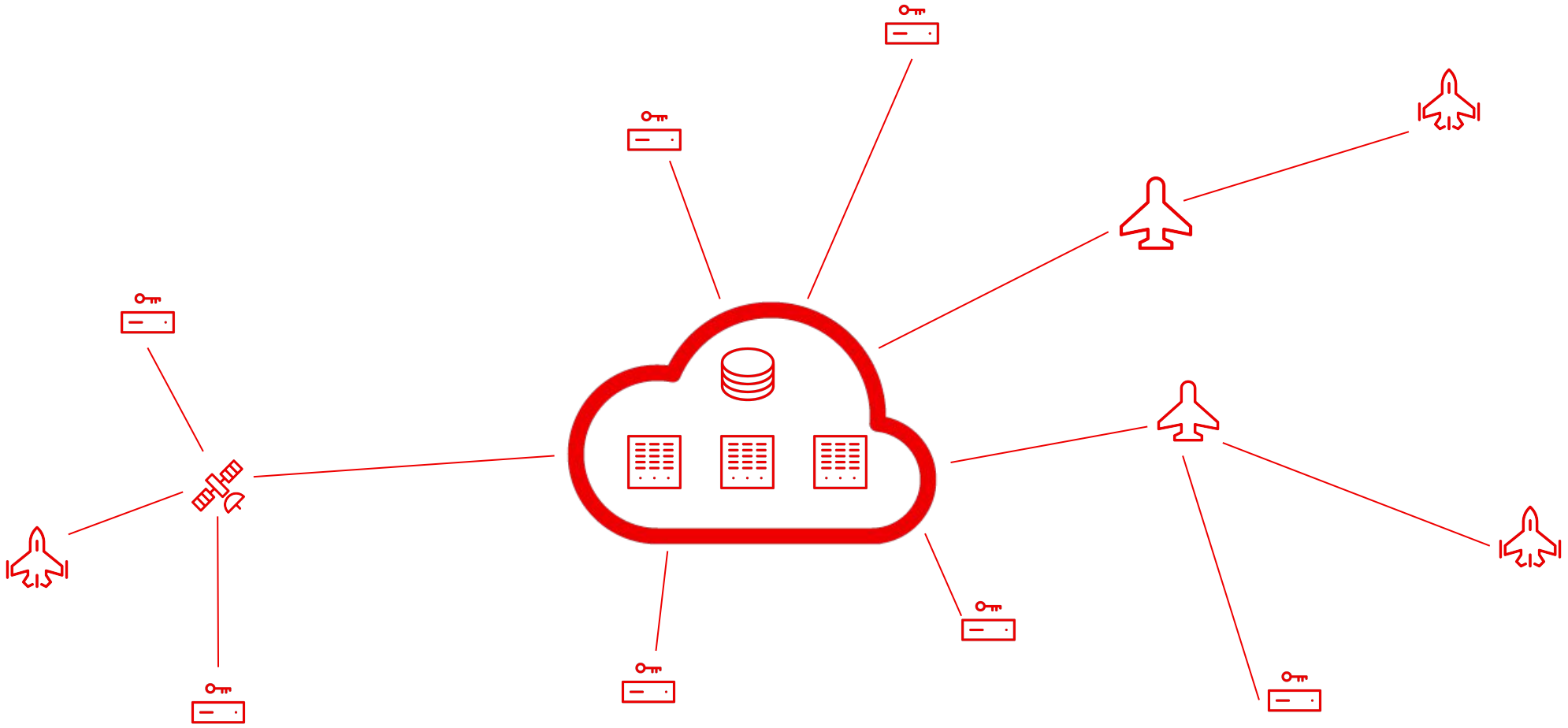
Updated: Aug 03, 2025 07:56 AM EST

Within the battlefield, units face multiple tactical risk scenarios

- Operating in disconnected comms environments
- Trusted device impersonation
- Compromised software in the field



Traditional Perimeter Security Fails



Operating in Degraded or Denied Environments

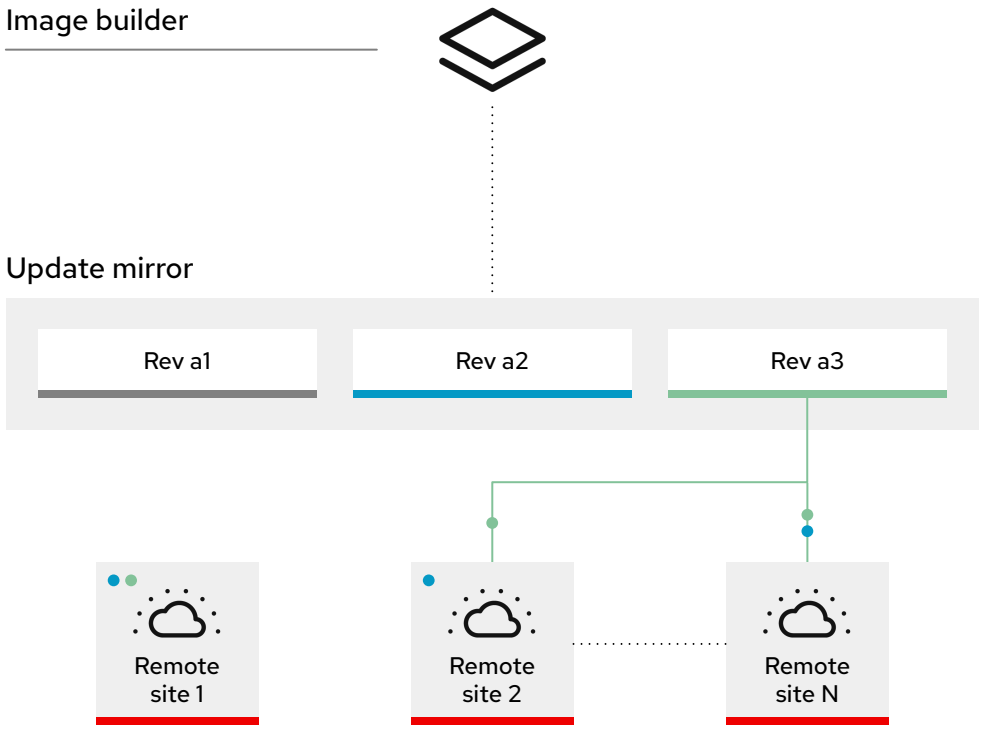
Local Authorization, Global Intent

Real-World Examples

Restricted and Disconnected

Operating in Degraded or Denied Environments

Efficient OTA updates, easy remote device mirroring, transfer only the deltas

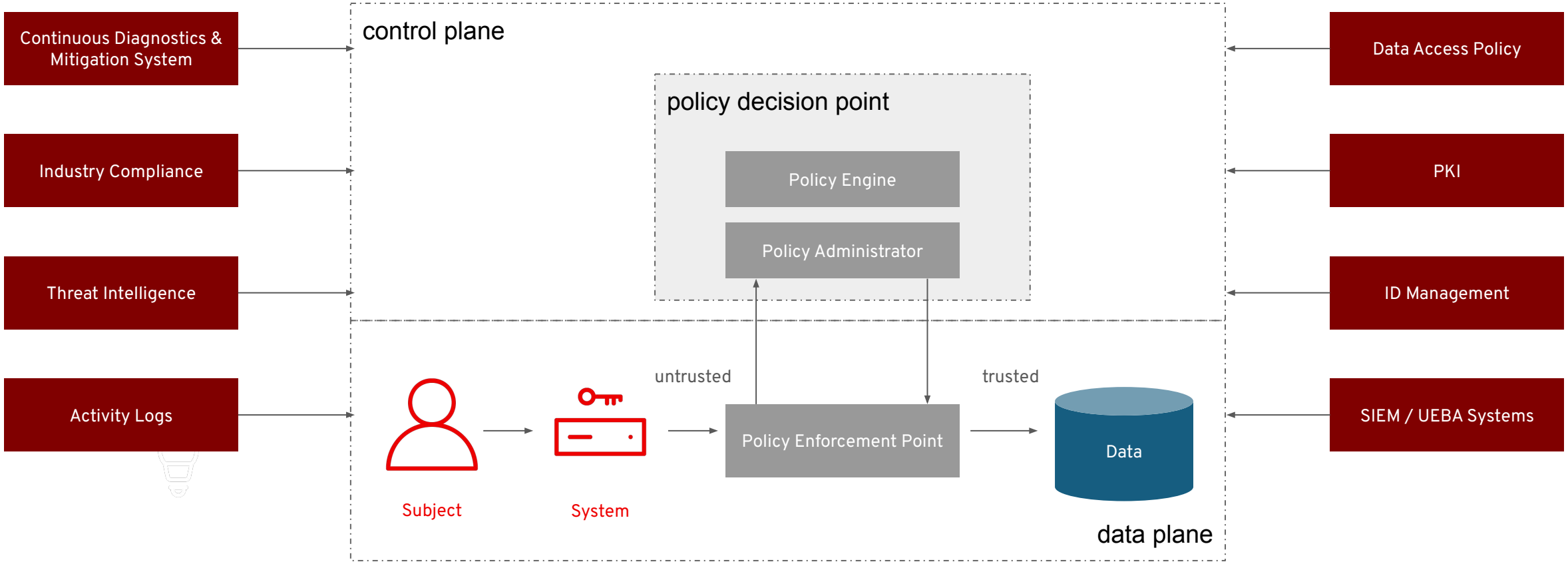


- Ideal for disconnected, intermittent, or low-bandwidth (DIL) connections
- Transfers significantly less data over the network*
- Only transfers updated bits of OS content
- Static-deltas can be created to further reduce network usage
- Client initiated connections for firewall-friendly experience

* When compared with traditional appliance image updates or individual package management strategies

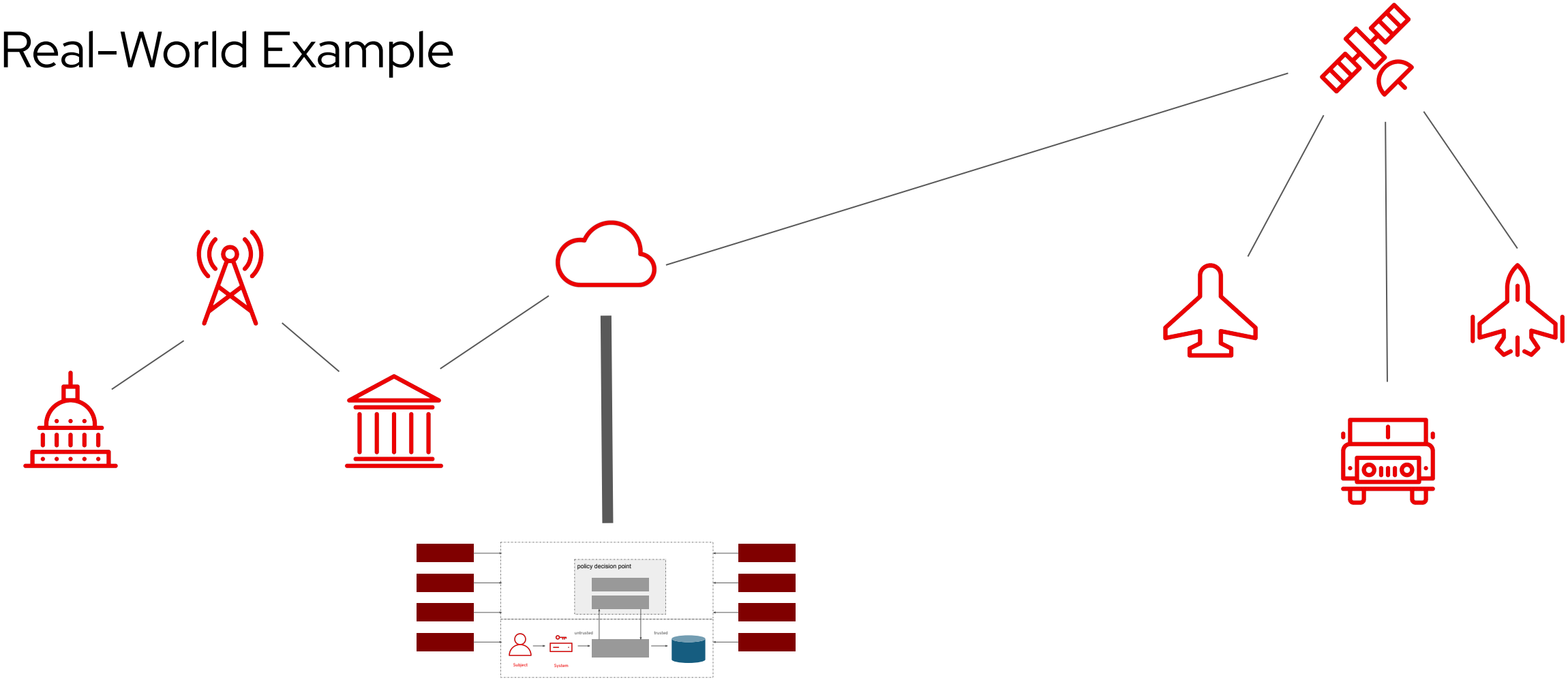
Local Authorization, Global Intent – syncing policies pre-deployment.

How to apply context to our access controls



Source:
NIST 207 https://csrc.nist.gov/publications/detail/sp/800-207/final

Real-World Example



What Are Immutable Containers?

Container Benefits

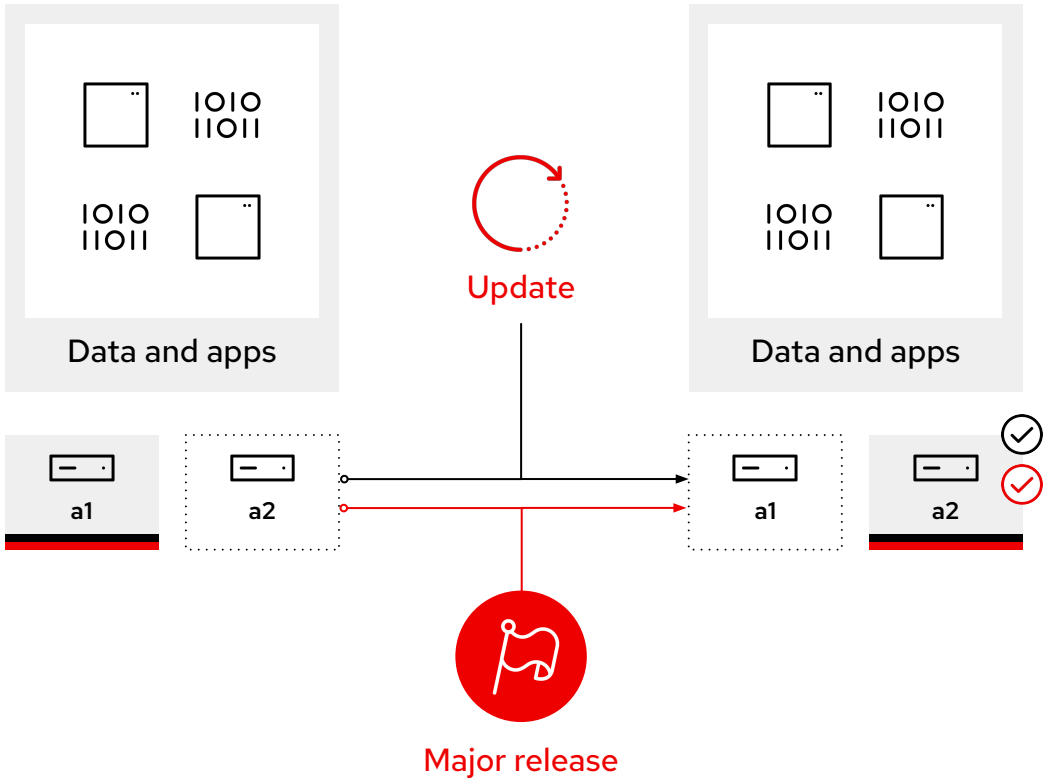
An Example Container “Stack”

Image Signing and Provenance

Containers and Immutability

What is immutability?

Immutable operating system (OS) and stateful configuration and storage

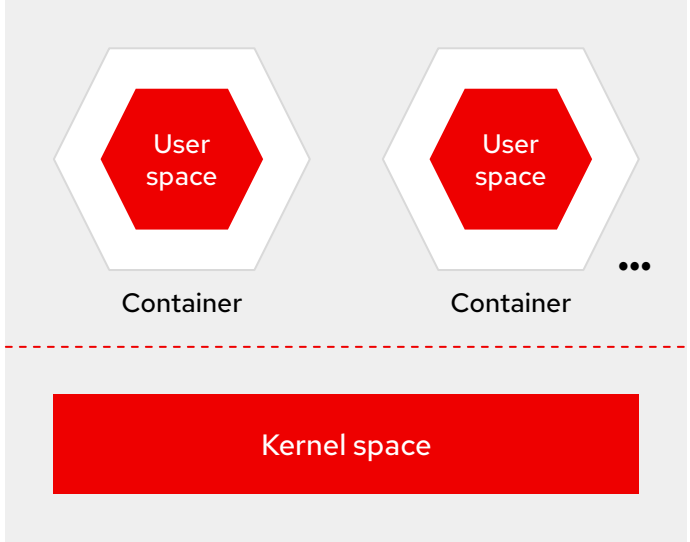


Transactional updates (A → B model)

- OS binaries and libraries are immutable and read-only
- State is maintained in restricted directories
- No in-between state during updates
- Updates are staged in the background and applied upon reboot
- Reboots can be scheduled with maintenance windows to ensure the highest possible uptime

Containers, managed by Podman

Provides benefits to Tactical Ops: consistency, rollback, reduced attack surface.



A container implementation without daemons

- Fast and lightweight
- Choice of runtimes*
- Standard container network interface (CNI) networking
- Remote management and cross-container compatibility via v2 API

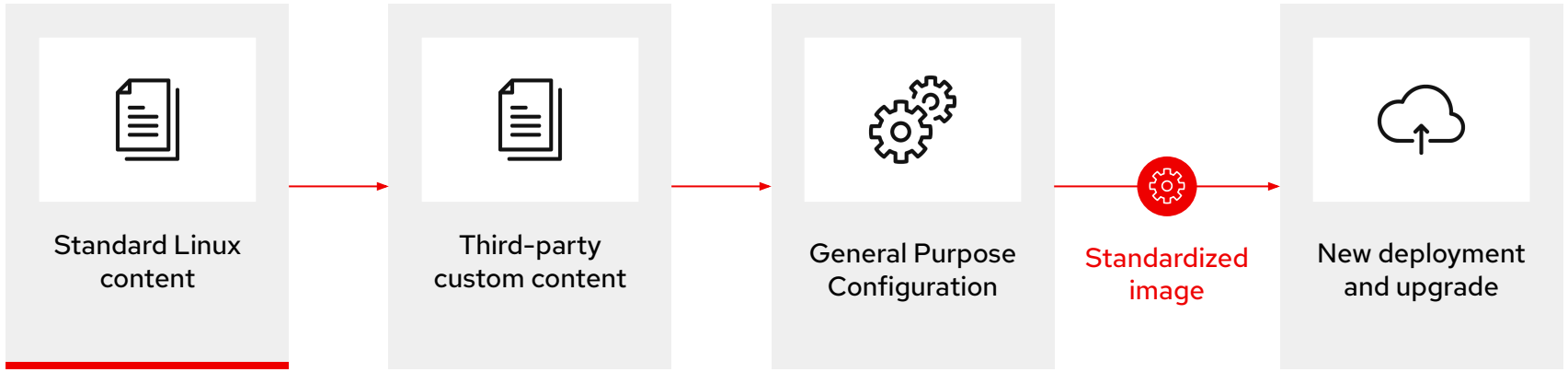
Native Linux technology

- Standards Compliant
- Additional container security
- Scheduling and process monitoring
- Auto-update based on registry tags, e.g :prod**

Typical Container Stack

lightweight container runtime + minimal base image.

Standardize your fleet with image sets to ensure uniform performance



Secure supply chain from source to build to deploy

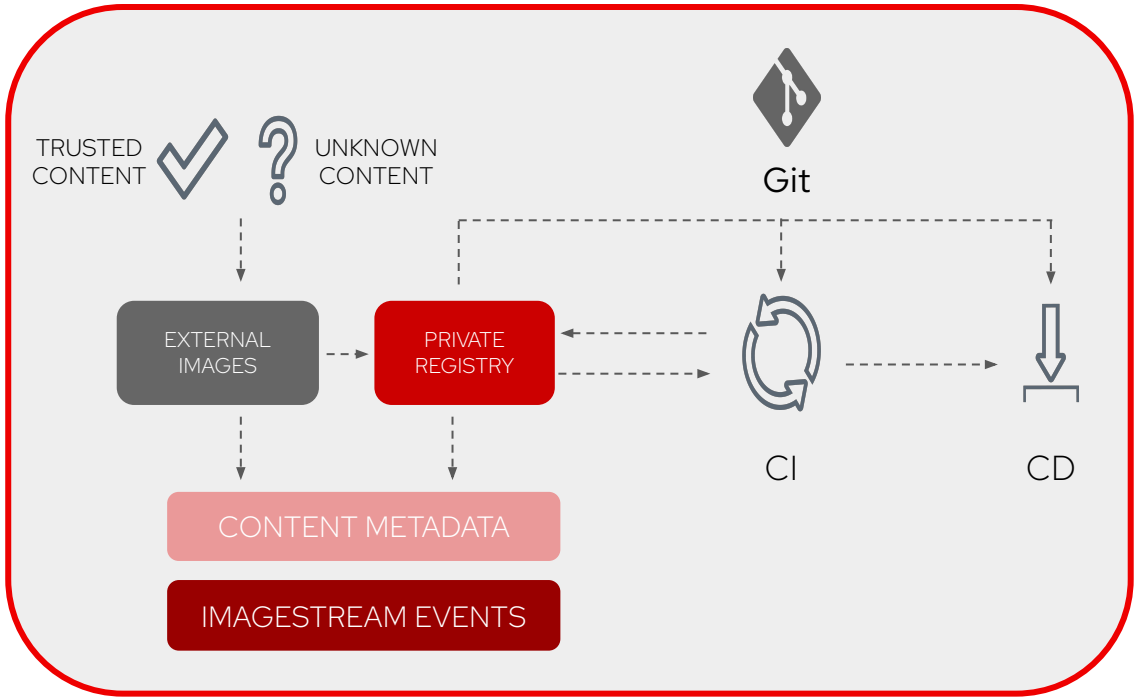
UBI
- Use signed and trusted sources for external content such as base images

Registry
- Use a trusted private registry to manage supply chain risk

Pipelines
- Automate your CI/CD pipeline to enable rapid updates

Registry scanner
Containerized IDE
Container Scanner
Linter
- Integrate security tools / gates in your pipeline to identify known vulnerabilities and application misconfigurations

Cluster Manager
- Use policy-based deployment tools to manage application placement (e.g. locality)



What is Policy-Based Security?

Open Policy Agent

Contextual Access Decisions

Enforcing Least Privilege in Real Time

Security Through Policy Enforcement

What is Policy-Based Security?

Policy-based security is a security model where rules (policies), rather than hard-coded configurations, define who can do what, under what conditions, and where.

- Policies are rules
- Security Decisions are separate from application code
- Can be enforced dynamically
- Managed centrally, enforced locally

OPA (Open Policy Agent) or Equivalent

Enforces the who / what / when / where

Open Policy Agent

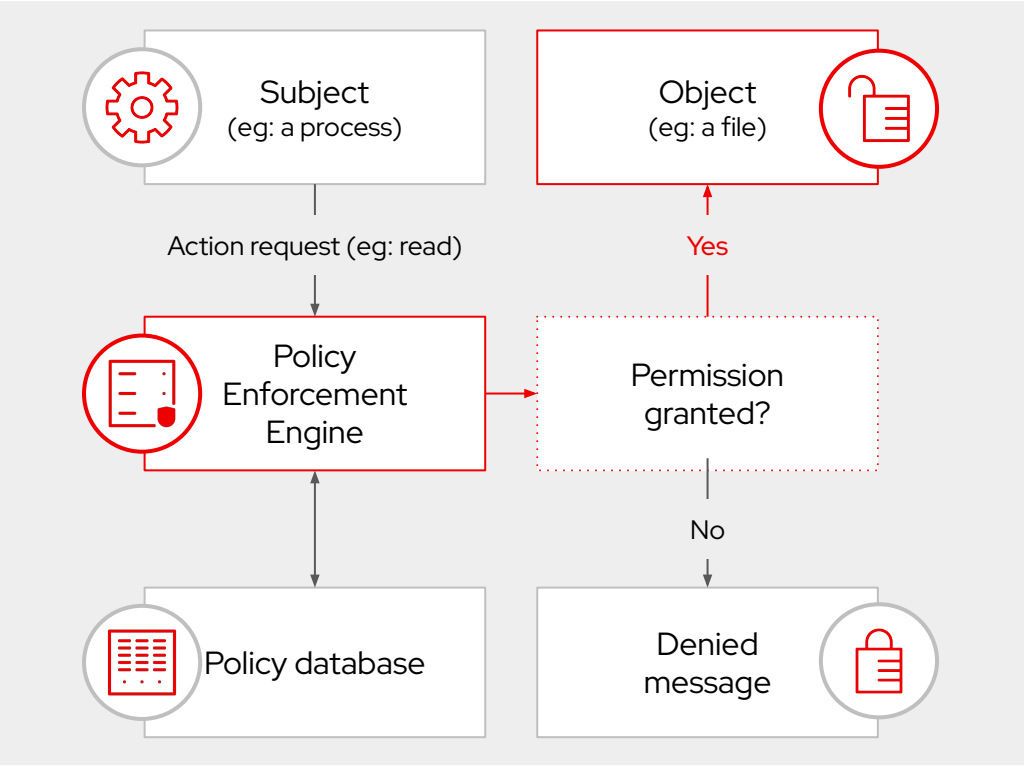
Developer Productivity: OPA helps teams focus on delivering business value by decoupling policy from application logic. Security & platform teams centrally manage shared policies, while developer teams extend them as needed within the policy system.

Performance: Rego, our domain-specific policy language, is built for speed. By operating on pre-loaded, in-memory data, OPA acts as a fast policy decision point for your applications.

Audit & Compliance: OPA generates comprehensive audit trails for every policy decision. This detailed history supports auditing and compliance efforts and enables decisions to be replayed for analysis or debugging.

Contextual Access Decisions

user identity + mission + posture



- Something requests to take an action
- Advanced process management, including Linux Containers (aka, Docker)
- Pluggable & Stackable Access Modules & IDM
- H/W and S/W identity and cryptographic attestations (via SecureBoot, KeyLime & TPMs, IMA, RH signing)
- Derivative operating systems via UBI, image builder, RHCOS to further minimize attack surface

Enforcing Least Privilege in Real Time

deny by default, allow via policy

policy.rego

```
package application.authz

# Only owner can update the device's information. Ownership
# information is provided as part of the request data from
# the application.
default allow := false

allow if {
    input.method == "PUT"
    some deviceid
    input.path = ["device", deviceid]
    input.user == input.owner
}
```

input.json

```
{
  "role": "operator",
  "owner": "tsgtsmith@af.mil",
  "path": [
    "fighters",
    "f15-1182"
  ],
  "user": "cmdrsmith@af.mil"
}
```

Why Automation Matters

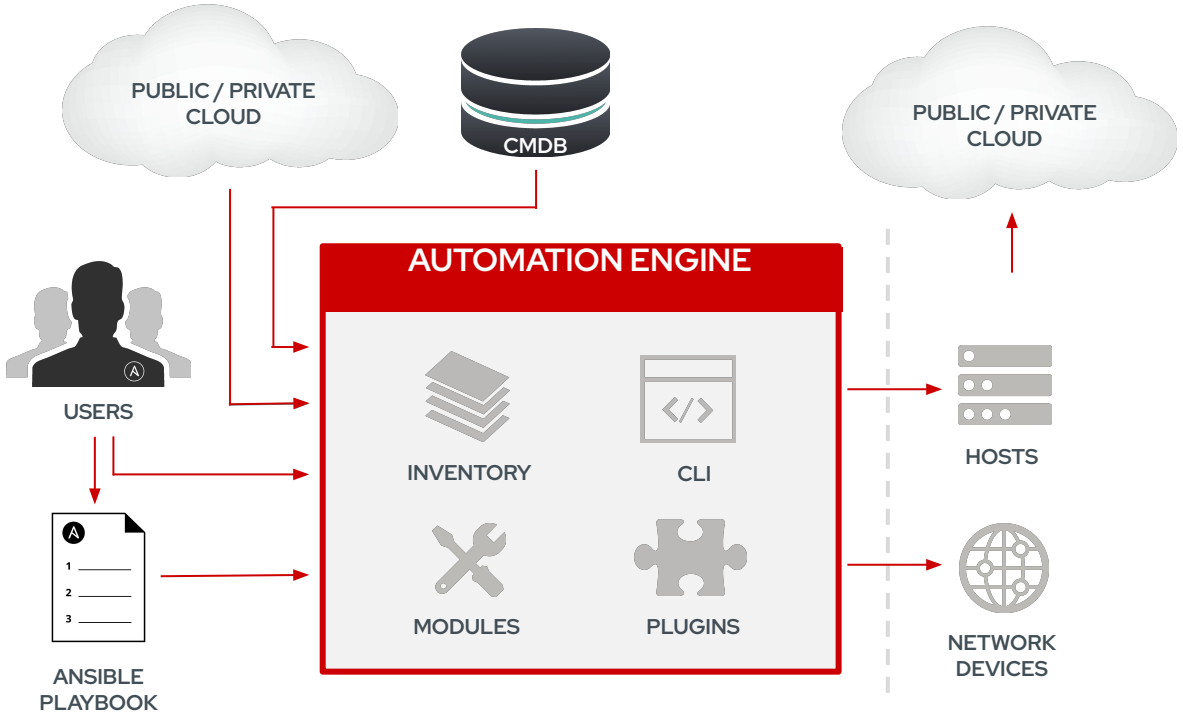
Role of Automation Platforms

Example Deployment

Scaling with Automation

Why Automation? Humans Cannot Scale Zero Trust

System automation is a requirement to push Zero Trust to the edge



System Automation delivers immediate ZTA capabilities:

- Inventorying systems, including hosts, networks, devices, and lots of other IT assets
- Applying security controls to your resources, throughout your enterprise and in all domains
- Single point of access and control that can be RBACed, logged, and audited

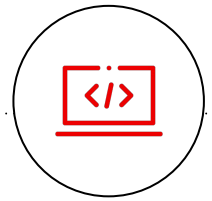
The role of automation is to mature and move us *faster*

Crawl

Opportunistic

How can we simplify a task or set of tasks?

- Infrastructure visibility
- Compliance
- Business continuity



Walk

Systematic

How do we centralise our processes?

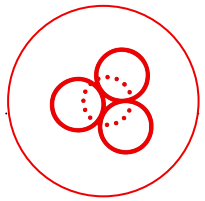
- Cloud operations
- Deployment and retirement
- Zero Trust

Run

Institutionalized

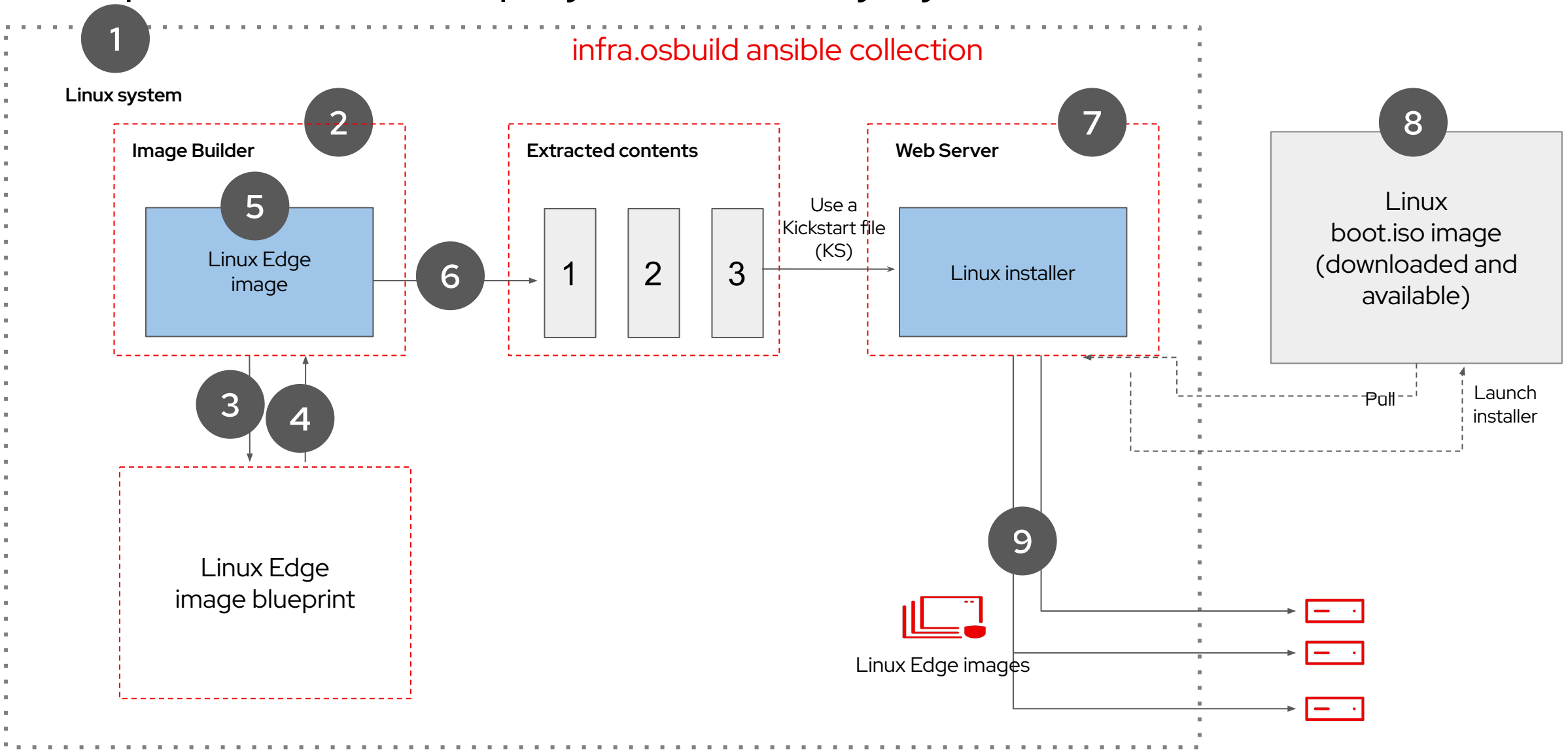
How do we orchestrate our processes

- Infrastructure optimization
- Infrastructure orchestration
- Automated troubleshooting



Increased complexity

Example Automatic Deployment + Policy Sync



Bringing Everything Together

Example Workflow

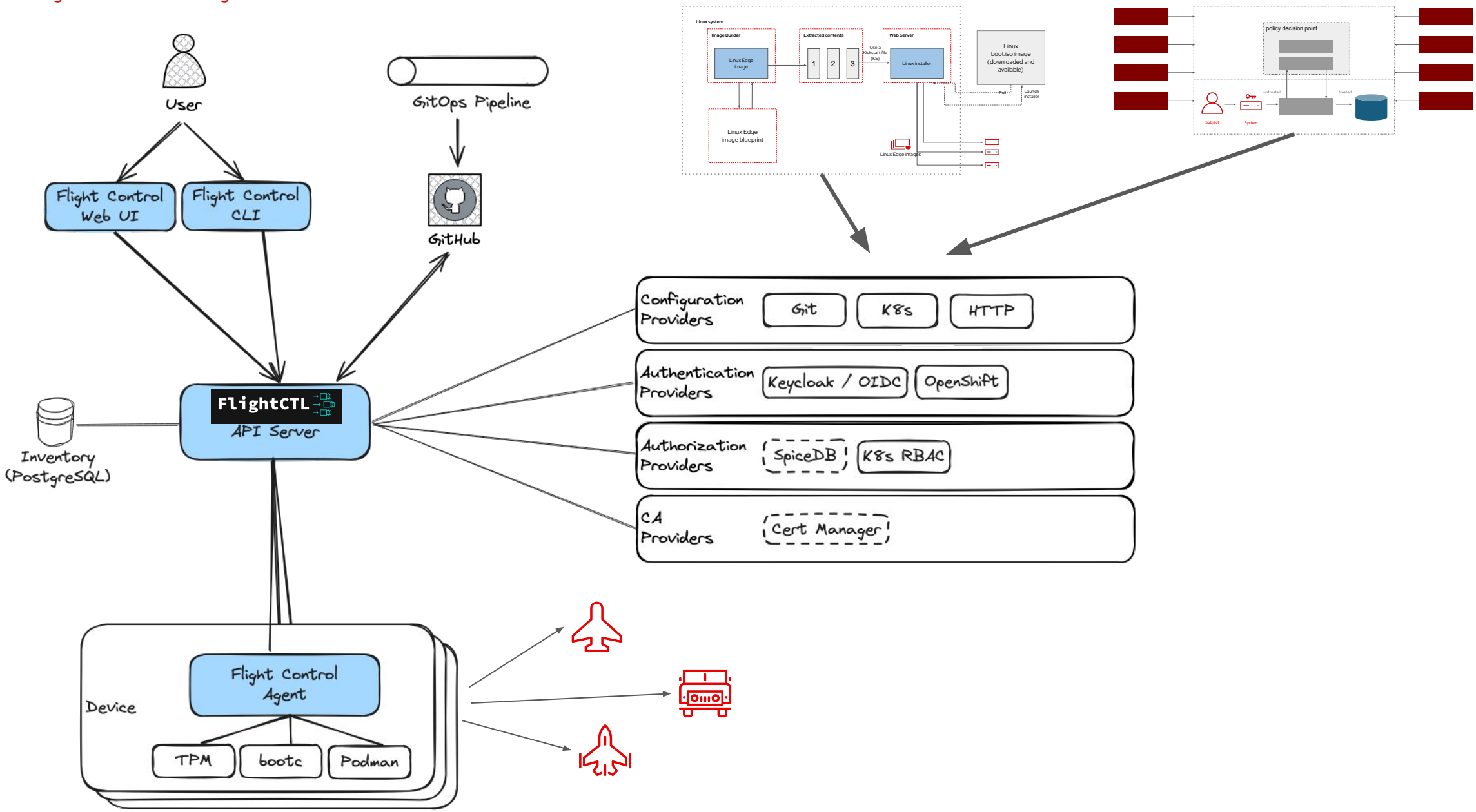
Airman-Centric Design

Pushing Zero Trust to the Edge

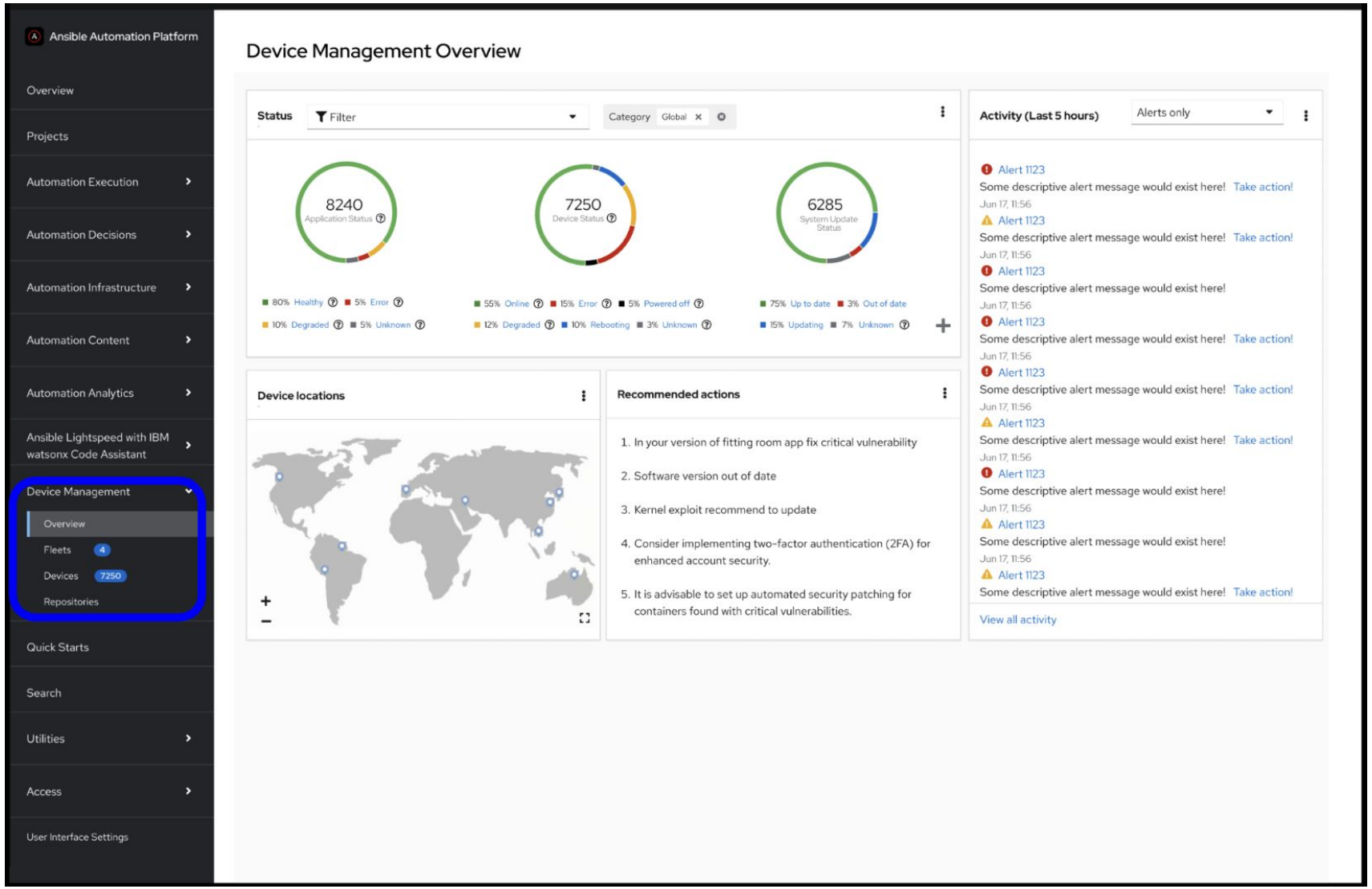
Bringing it together: Flight Control, an Edge Device Manager

- Simplified, secure onboarding of edge devices, streamlining fleet-scale deployments.
- Declarative GitOps-based management for OS, configuration, and application lifecycle across devices.
- Fleet-level management templates and rollout policies with status aggregation across devices.
- Resilient agent-based architecture for:
  - Seamlessly manage devices across private and mobile networks under varying conditions, without relying on VPN or SSH.
  - Secure over-the air (OTA) updates with verification and intelligent rollback capabilities.
  - Lightweight, continuous device and app monitoring.
- Product documentation

Pushing Zero Trust to the Edge



Airman-Centric Design: global view, granular control, simplified field ops



The Digital Security Threat is Real

Network Degradation is a Reality

Containerization Can Empower Zero Trust

Control The Environment With Policy

Scale Zero Trust With Automation

Get to the Edge With Flight Control

Closing Thoughts

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat