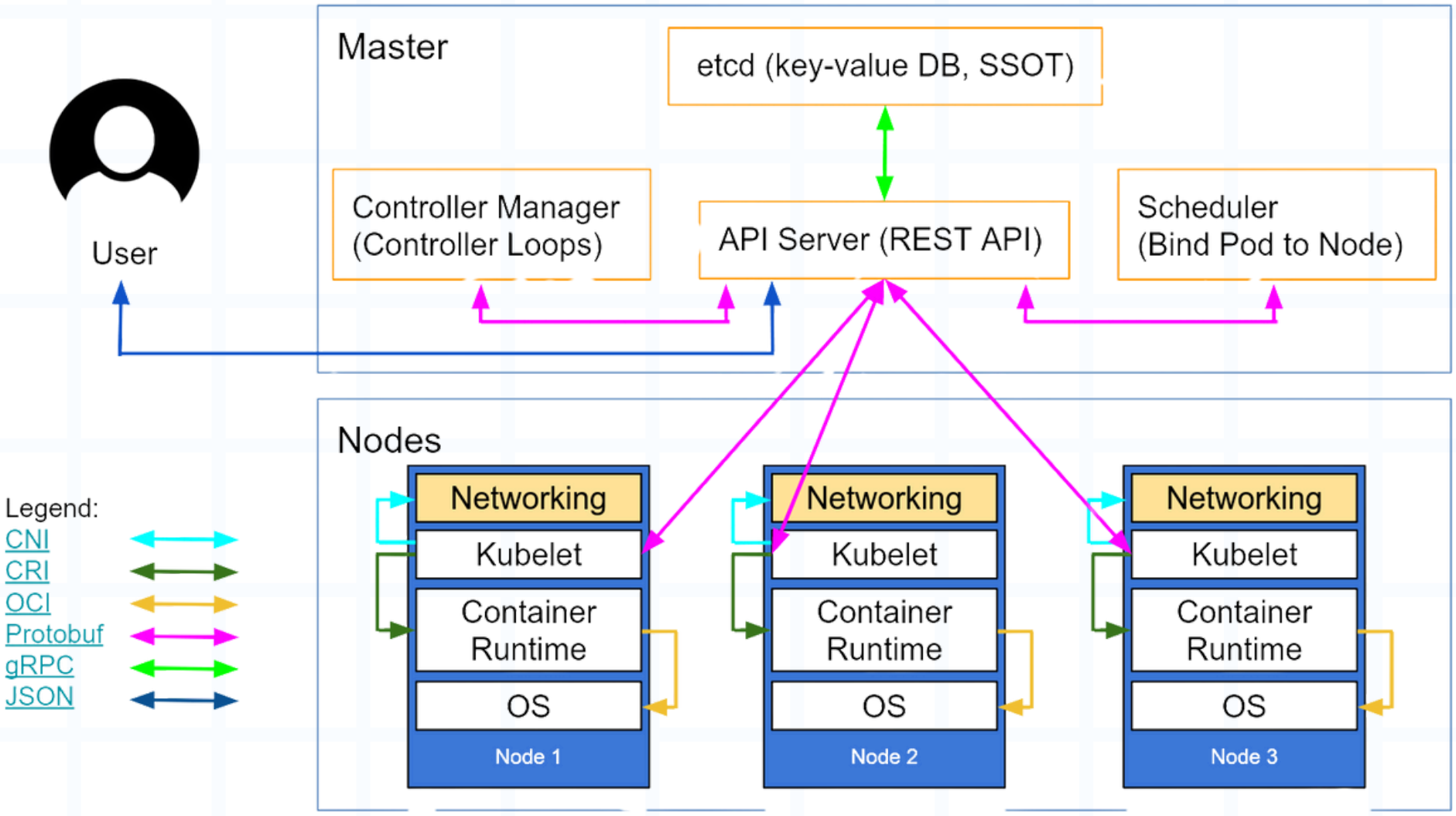
Jaswindder
Director of Cloud Strategy, DevOps and Security

11 Ways (Not) to Get Hacked.

Jaswindder
Director of Cloud Strategy, DevOps and Security

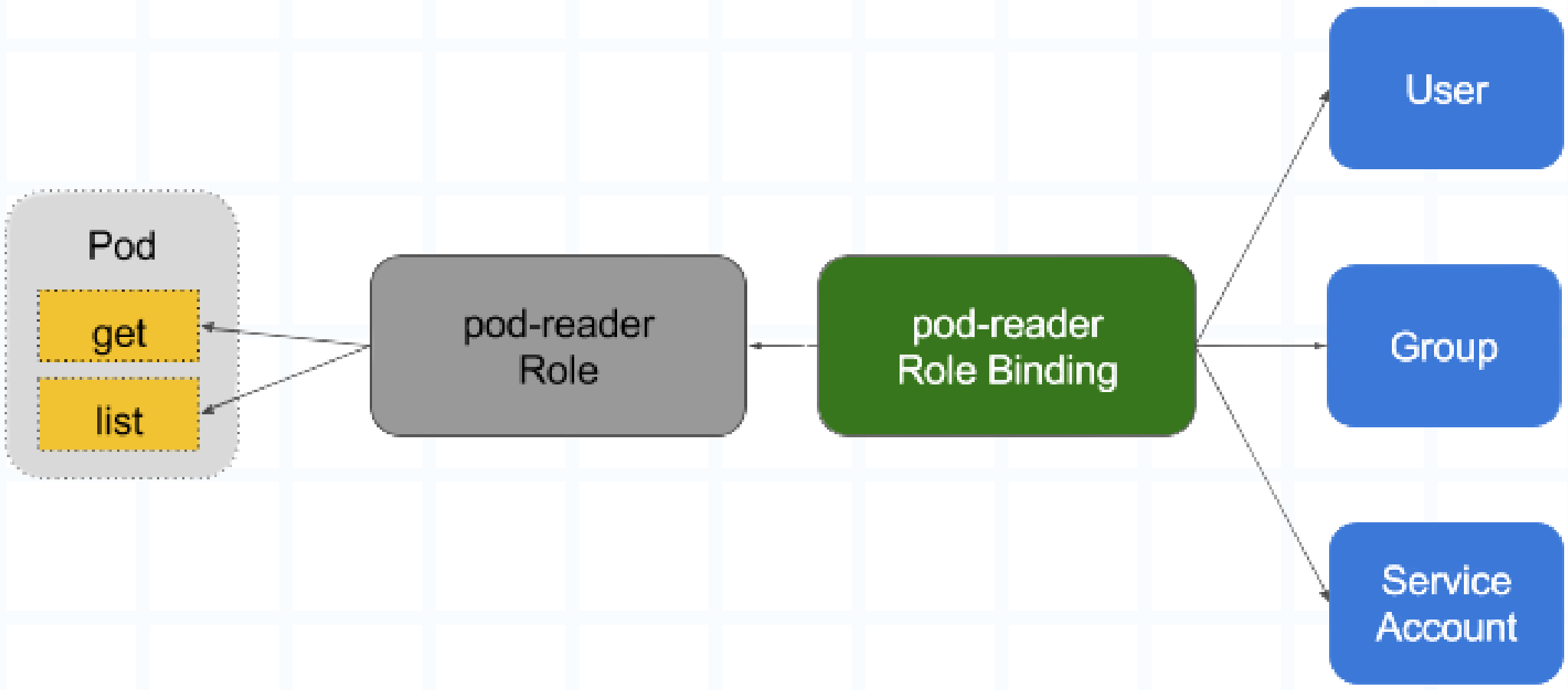
1. Use TLS Everywhere



- Encrypt all the traffic between Kubernetes components.
- Imagine if every room in your house had a locked door no one could secretly overhear or tamper with conversations.
- This keeps hackers from “listening in” or faking communication inside your system.

Jaswindder
Director of Cloud Strategy, DevOps and Security

2. Enable RBAC, Disable BAC, and Monitor Logs



- RBAC = Role-Based Access Control → give people only the permissions they truly need.
- Stop using outdated ABAC, which is too broad and risky.
- Always ship logs to an external system and monitor them think of it like 24/7 CCTV footage for your cluster.

Jaswindder
Director of Cloud Strategy, DevOps and Security

3. Use Third-Party Authentication for the API Server

- Don’t reinvent the wheel with custom login systems.
- Plug into trusted platforms (Google, GitHub, Active Directory, etc.) to safely verify user identities.
- Centralized authentication means less risk of weak or fake accounts slipping in.

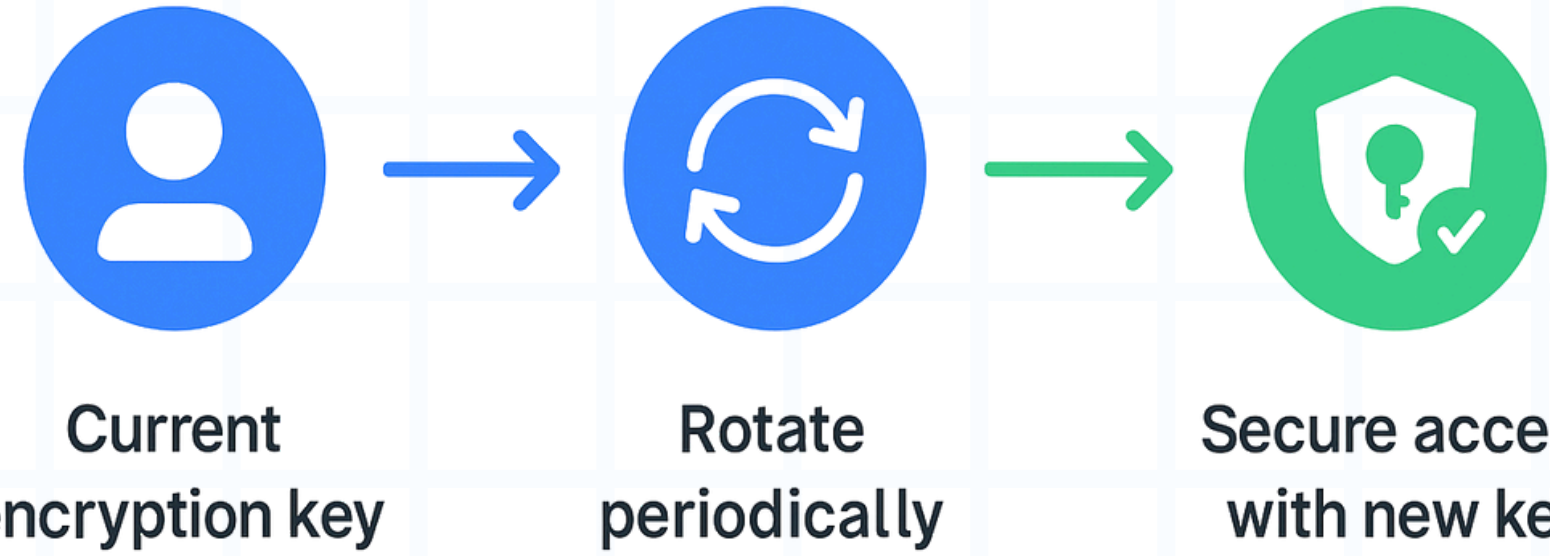
Jaswindder
Director of Cloud Strategy, DevOps and Security

4. Separate and Firewall Your etcd Cluster

- etcd is the memory and brain of Kubernetes—it stores all the important state.
- If attackers get into etcd, they own your cluster.
- Keep it isolated on its own servers, protect it with TLS, and add firewall rules to block unwanted access.

Jaswindder
Director of Cloud Strategy, DevOps and Security

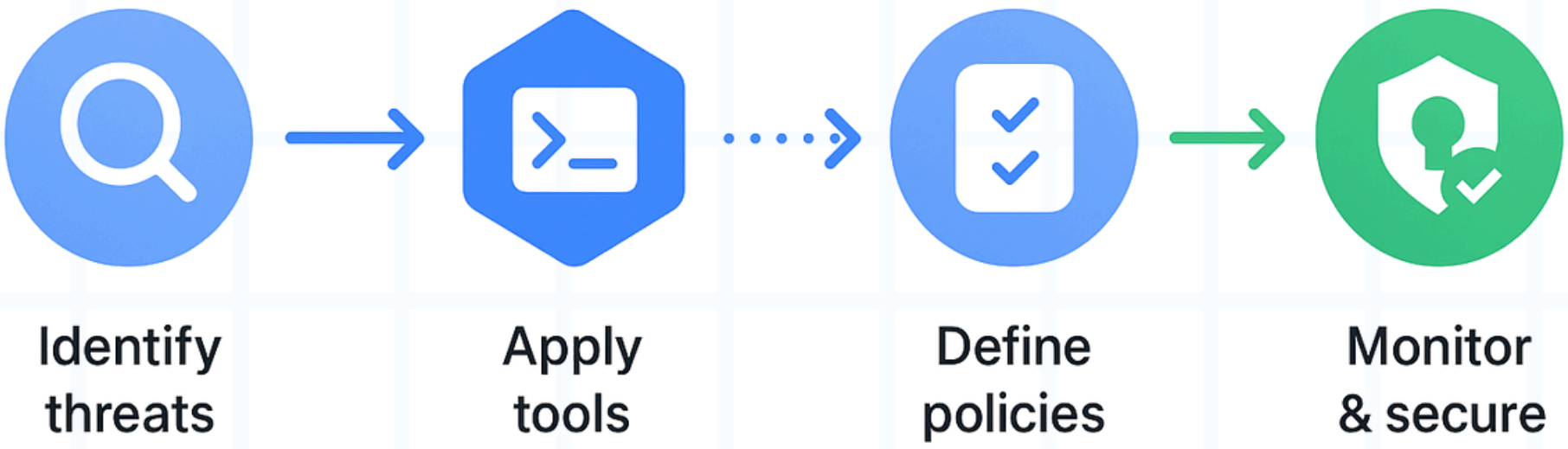
5. Rotate Encryption Keys Regularly



- Encryption keys = house keys to your cluster.
- If a key gets leaked, an attacker can walk right in.
- Rotate keys and certificates often, so stolen ones become useless quickly.

Jaswindder
Director of Cloud Strategy, DevOps and Security

6. Use Linux Security Tools and Pod Security Policies



- Add multiple “locks” at the container level.
- Tools like SELinux, AppArmor, and seccomp limit what a container can do.
- Even if hackers get in, their movements and actions are tightly restricted.

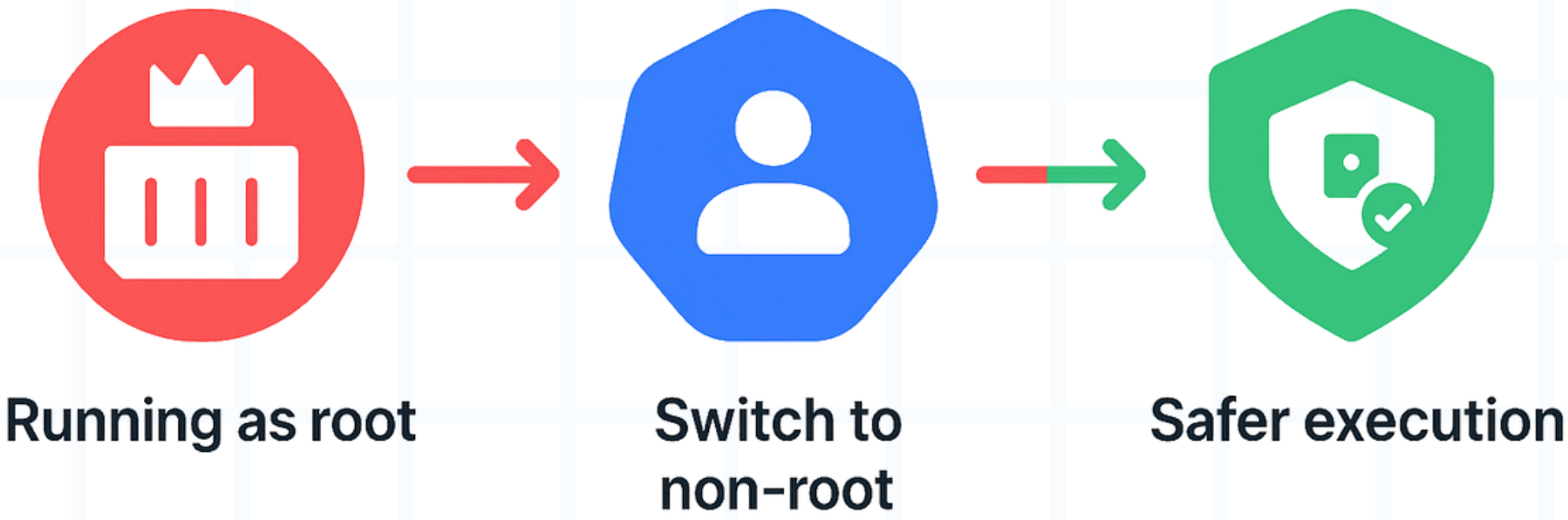
Jaswindder
Director of Cloud Strategy, DevOps and Security

7. Statically Analyze YAML Files

- YAML files tell Kubernetes how to run your apps.
- One wrong config can expose secrets or give more power than intended.
- Use tools that scan YAML before deployment catching mistakes before hackers can exploit them.

Jaswindder
Director of Cloud Strategy, DevOps and Security

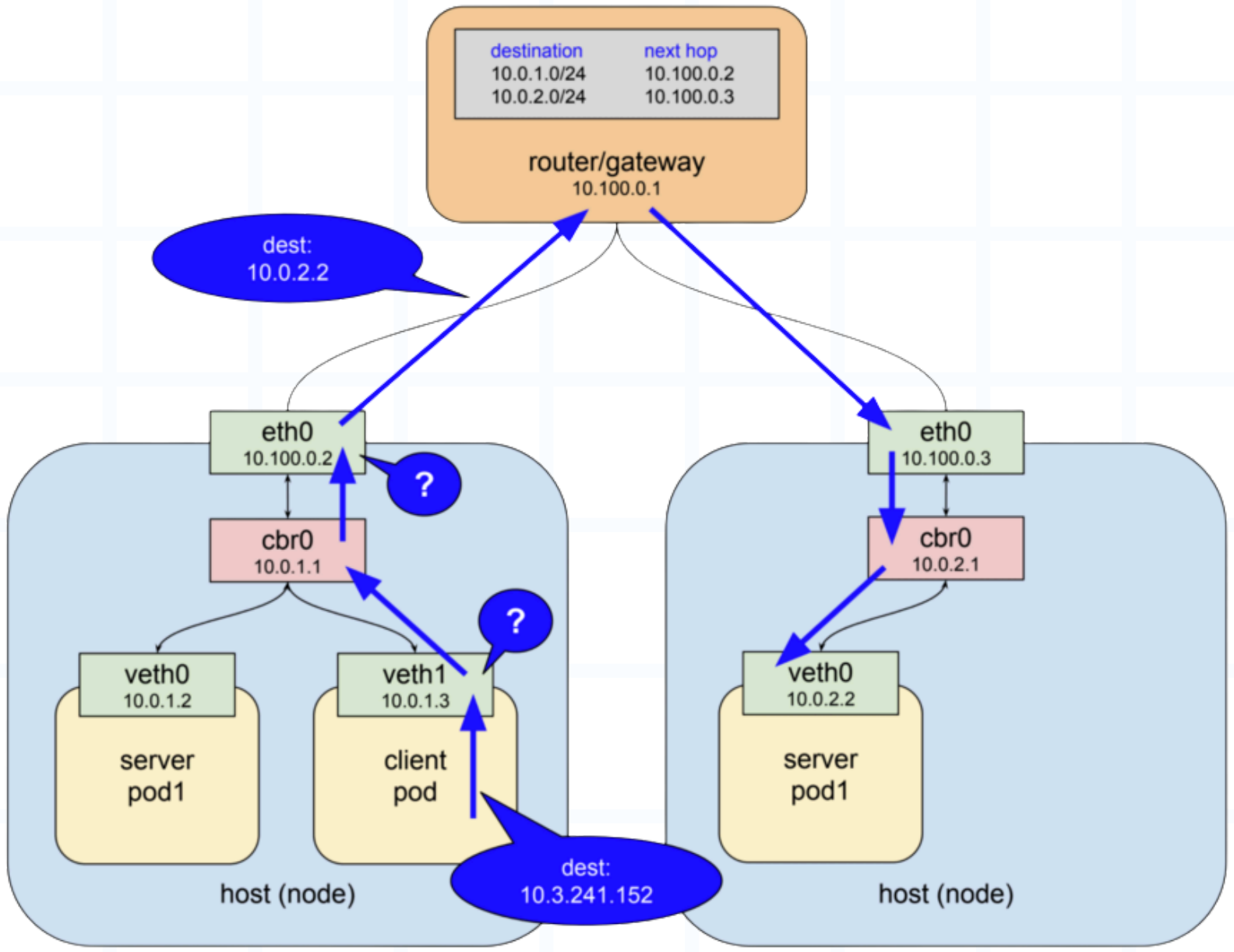
8. Run Containers as Non-Root Users



- Containers often run as “root” (admin), which is dangerous.
- Make them run as regular users instead.
- That way, if one container is hacked, it can’t spread damage across the whole cluster.

Jaswindder
Director of Cloud Strategy, DevOps and Security

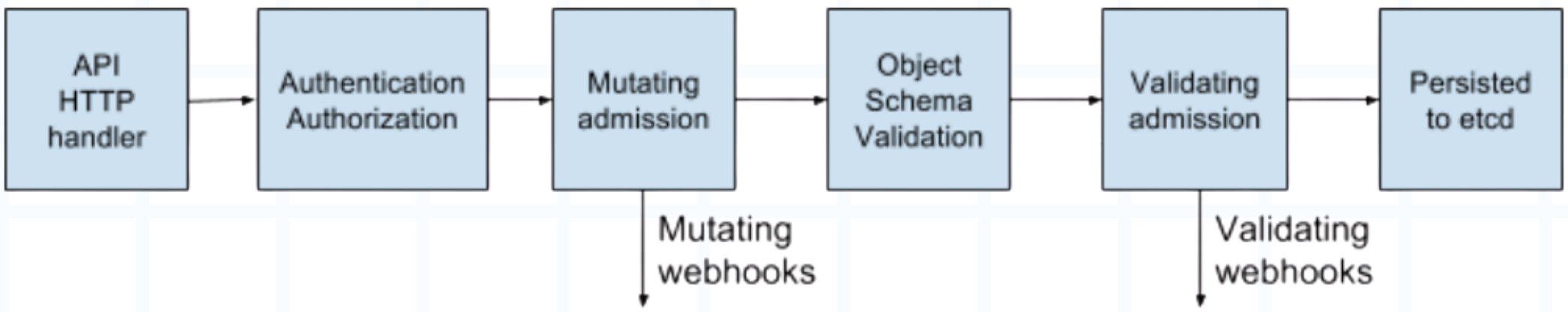
9. Use Network Policies



- Think of it like building walls and doors inside your house.
- By default, pods can talk to each other freely—that's risky.
- Network Policies let you decide who can talk to whom, stopping attackers from moving sideways across the system.

Jaswindder
Director of Cloud Strategy, DevOps and Security

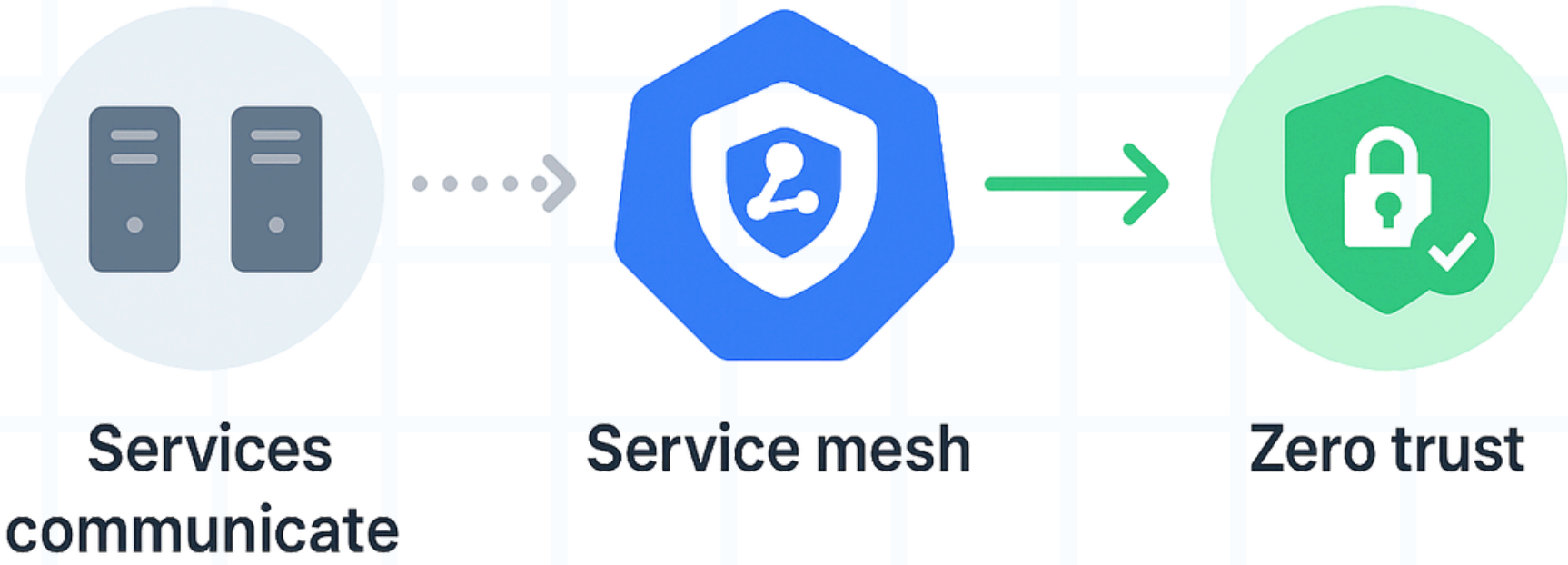
10. Scan Images and Use Intrusion Detection



- Container images can hide malware or outdated software.
- Regularly scan them before running.
- Add intrusion detection systems (IDS) that raise alarms when something suspicious happens—like an antivirus for your cluster.

Jaswindder
Director of Cloud Strategy, DevOps and Security

11. Run a Service Mesh



- Tools like Istio or Linkerd add an extra security guard between services.
- They automatically encrypt traffic, enforce rules, and provide visibility.
- This creates a “zero trust” environment where no service is trusted by default.

Follow for expert Cloud, DevOps & Security insights

Jaswindder Kummar

Director of Cloud Strategy, DevOps and Security

Follow