SECURING CLOUD WORKLOADS AT SCALE

Nick Jones

F-Secure

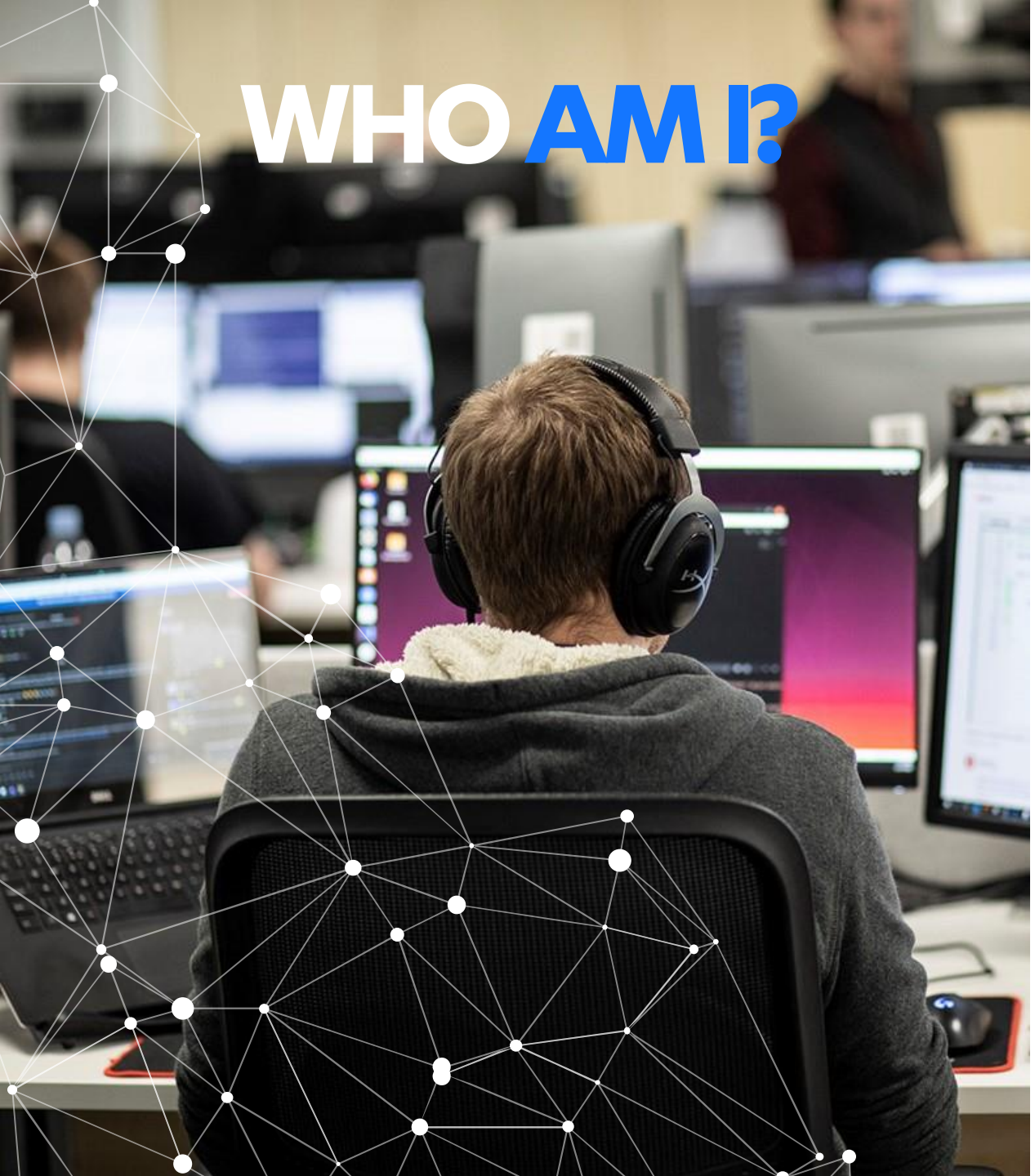
THIS PRESENTATION WILL COVER...

What your cloud security landscape really looks like

How an attacker target your workloads

The key security controls to have in place

F-Secure



NICK JONES

- Cloud Security Lead @ F-Secure Consulting
- AWS Community Builder
- Presented at DEF CON, fwd:CloudSec, RSA, t2, DevSecCon etc

F-SECURE CONSULTING

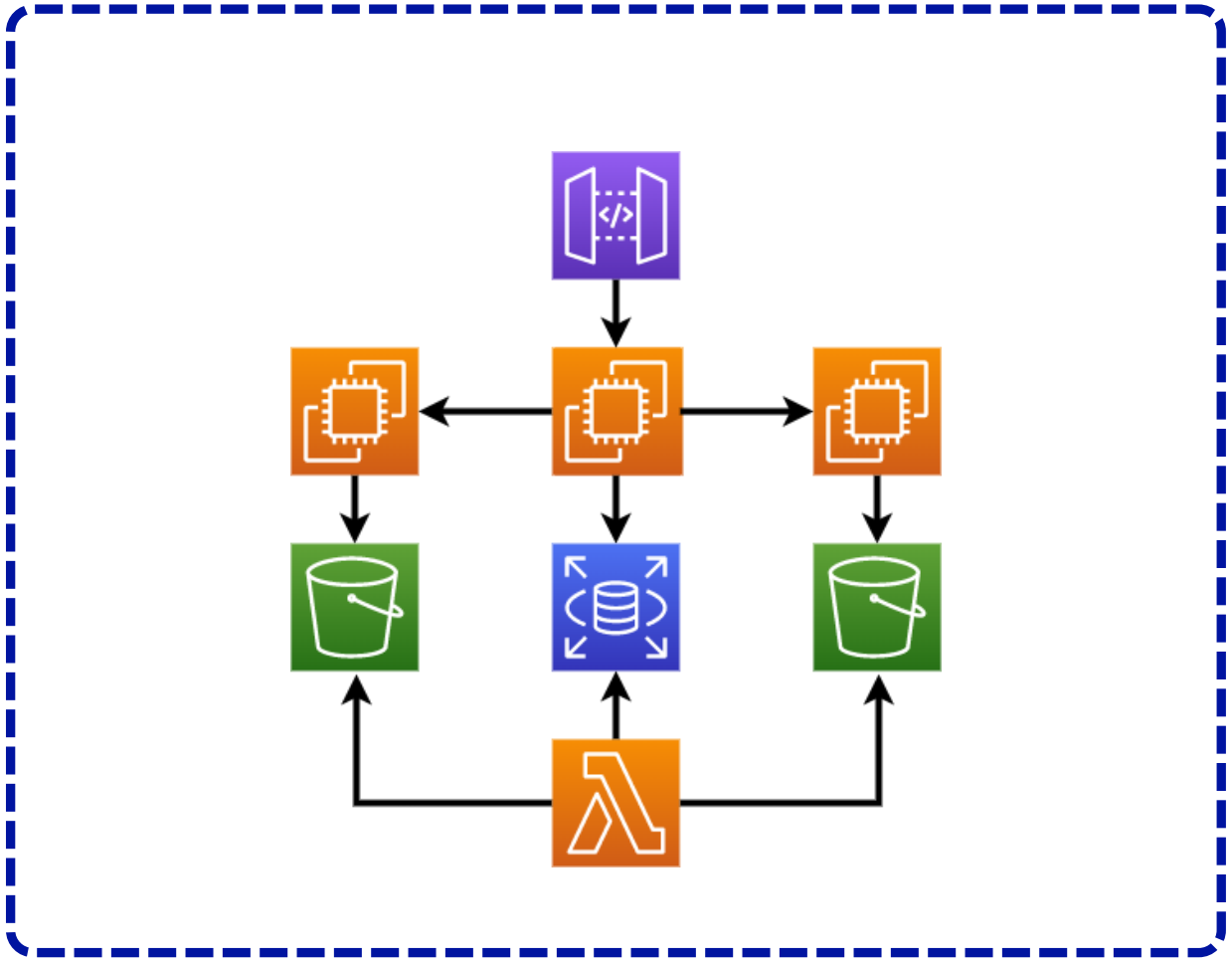
- Global cybersecurity consultancy
- >16 years experience across 8 countries

F-Secure

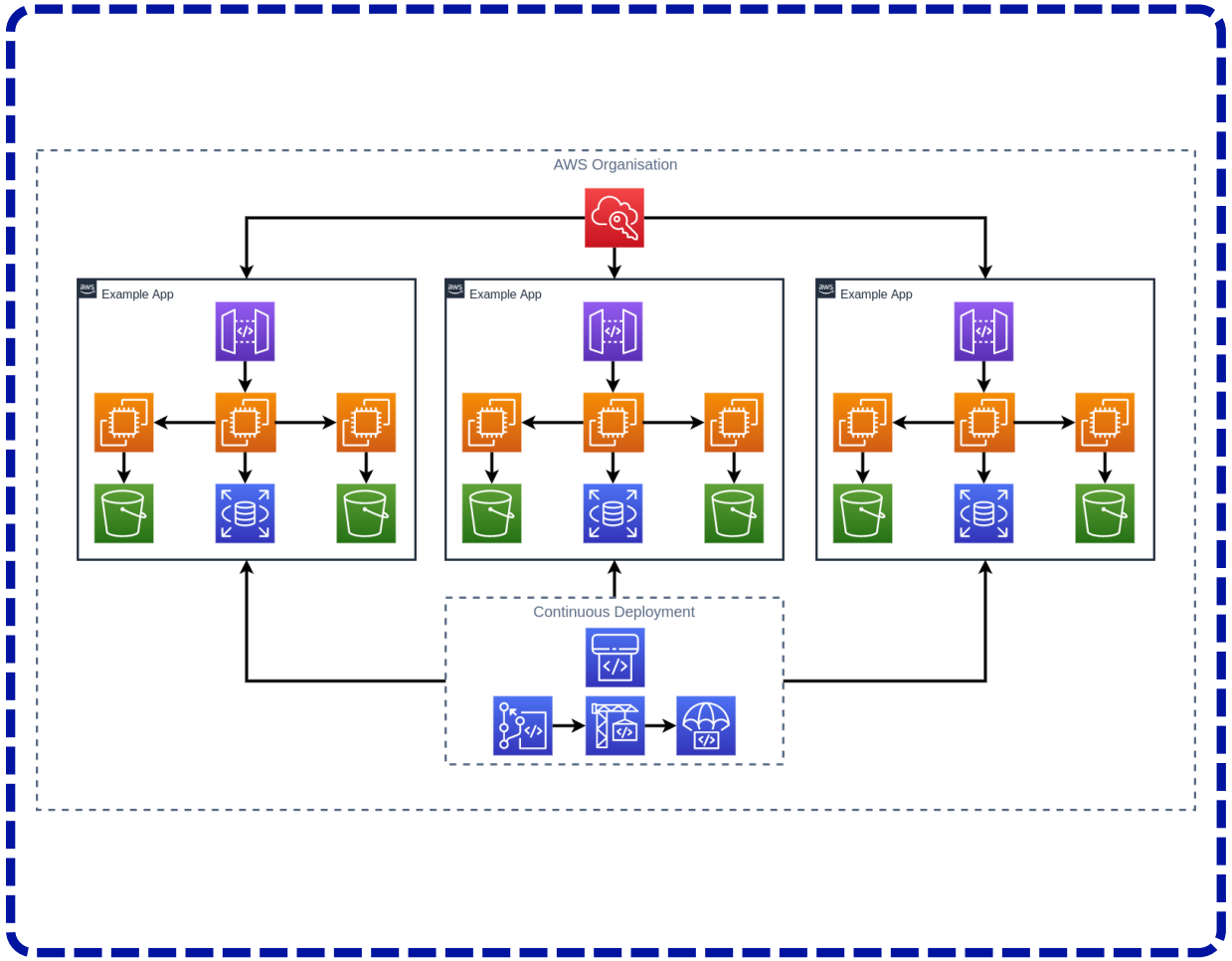
WHAT DOES YOUR SECURITY LANDSCAPE LOOK LIKE?

F-Secure

TYPICAL SCOPE FOR SECURITY MODELLING

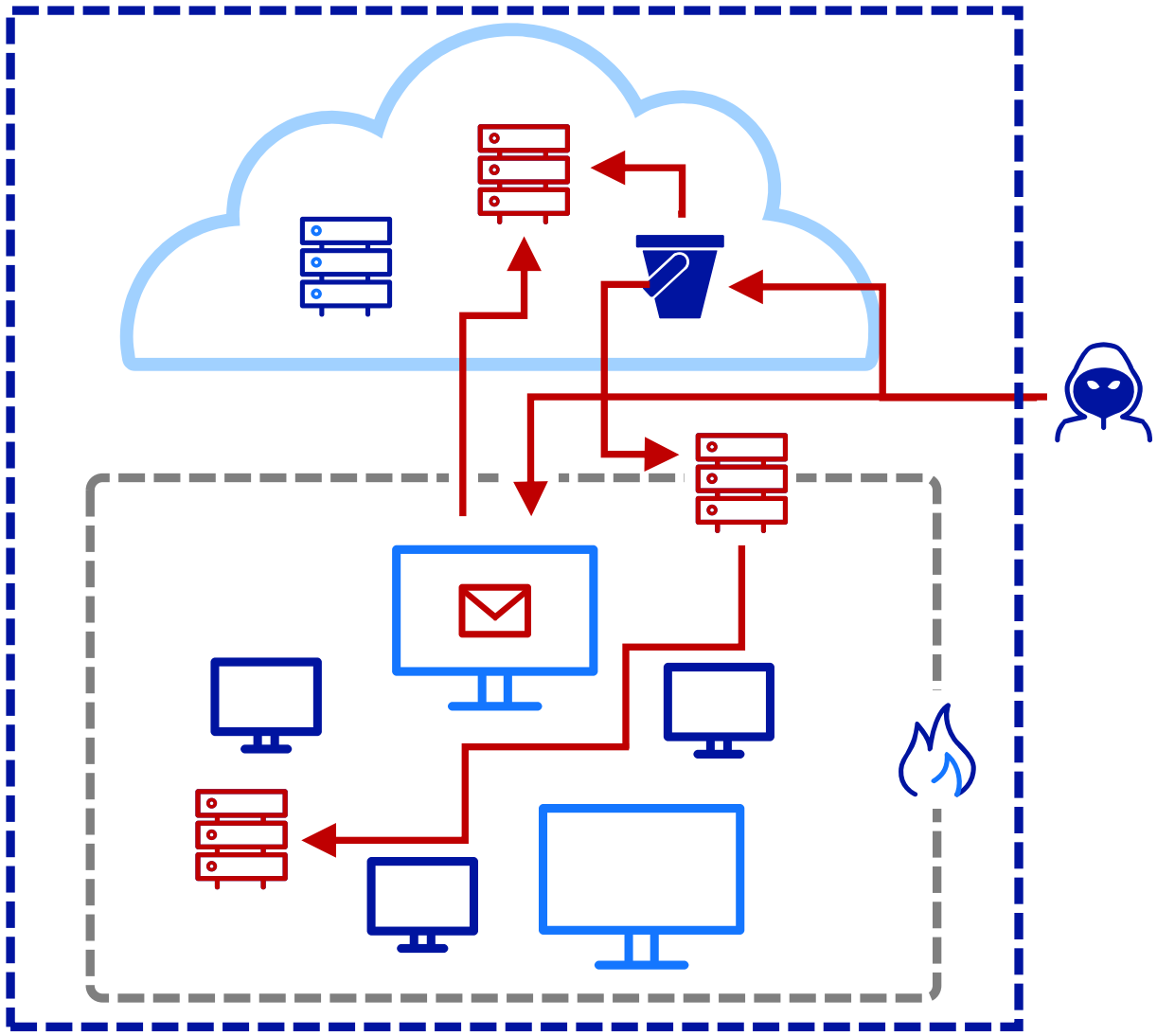


REAL SCOPE FOR SIMPLER ENVIRONMENTS



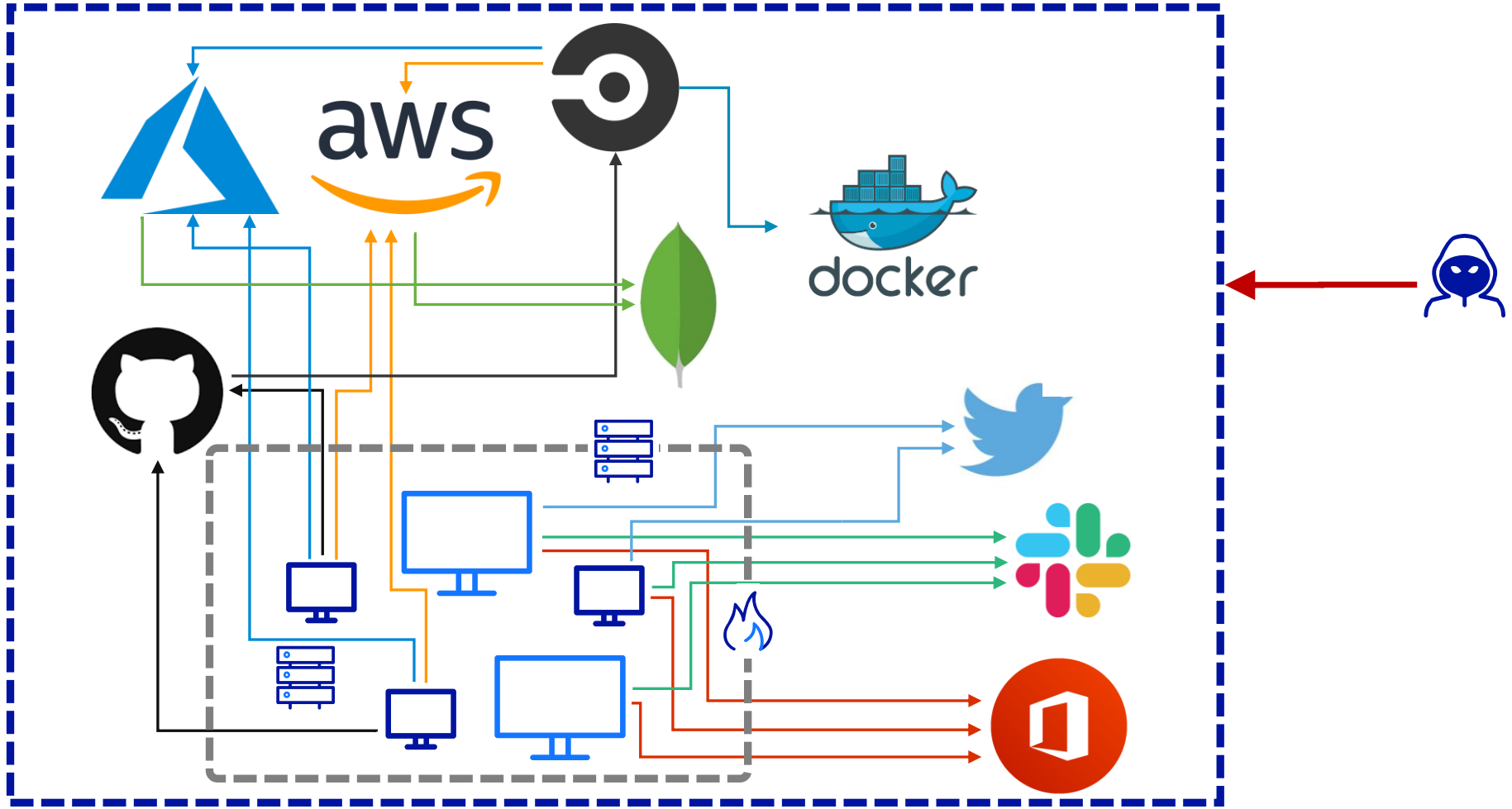
F-Secure

REAL ATTACKERS DON'T JUST ATTACK THE CLOUD



F-Secure

THE REALITY



SHIFTING VULNERABILITY CLASSES

- Shared responsibility model means loss of visibility and control
- Segregation now largely by identity, not network location
- Lots of old issues go away, become the provider's problem, or reduce in impact
- Mindset shift needed, from vulnerabilities to misconfigurations

F-Secure

DEVOPS CHANGES THE SECURITY PROCESSES

Mature organisations doing DevOps right deploy frequently	How do you assure the security of a constantly changing environment?	How do you perform forensics in the cloud?
▪ Netflix – hundreds/thousands of times a day ▪ Amazon – every ***11.7 seconds*** on average	▪ How do you do vulnerability scanning when systems appear/disappear mid-scan? ▪ How do you penetration test an app that changes multiple times a week?	▪ Systems may not exist any more by the time a breach is detected ▪ No clear guidance on how underlying technology affects typical data collections

COMPOSITION OF SYSTEMS

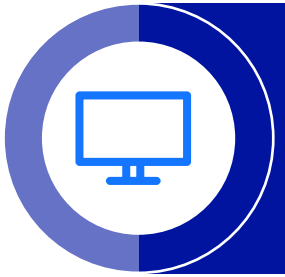
Monolithic systems are giving way to microservices

"Cloud native" deployments make extensive use of PaaS

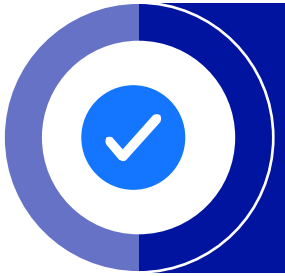
Connection points between systems more important than ever

Exacerbates existing secrets management issues

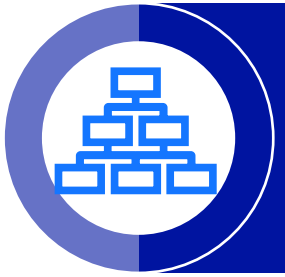
NO PERIMETER / 'ZERO TRUST'



There is no longer a big firewall around your perimeter



Less defence in depth than was common historically



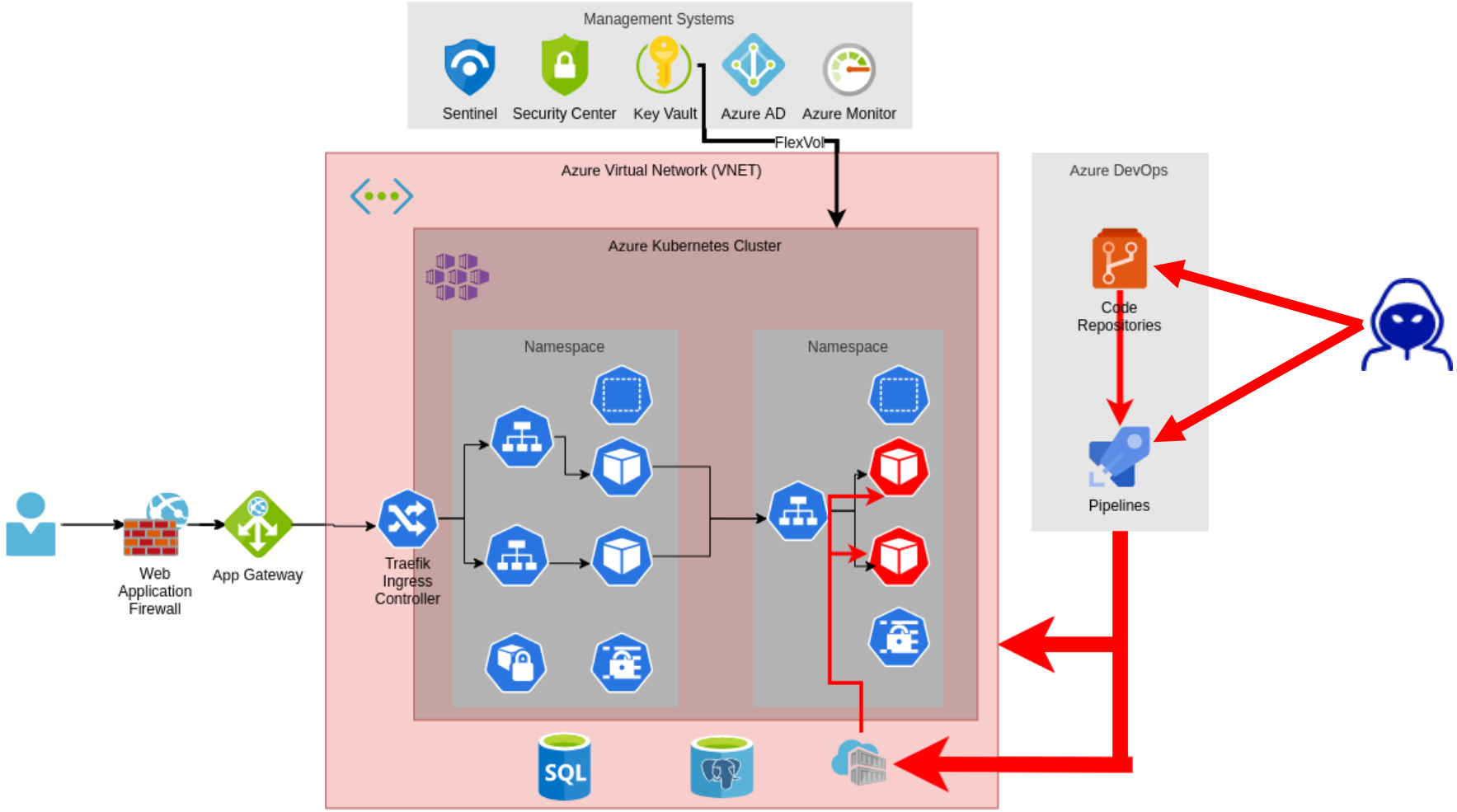
People moving towards a "zero trust networking model"

Services don't trust each other, other than some central, strong auth system

No more VPNs – expose everything to the internet

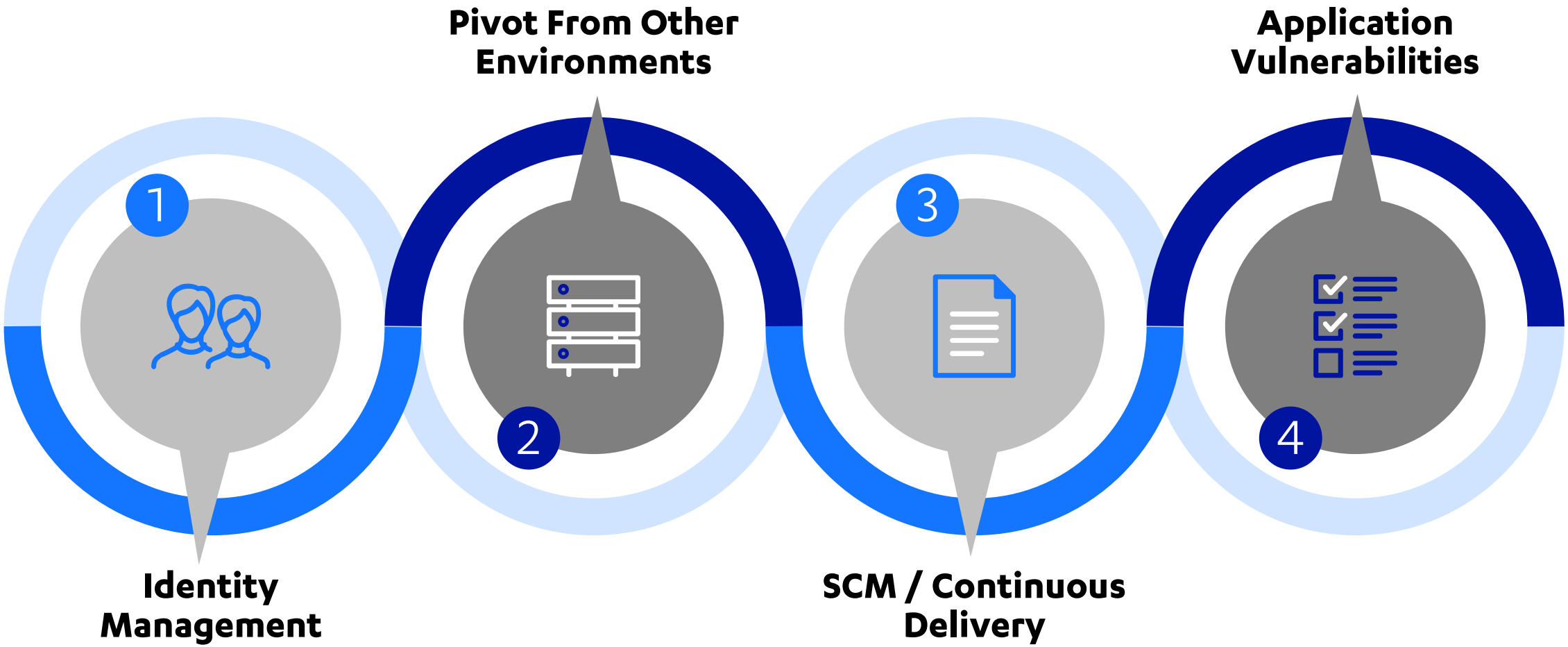
Works for Google, why shouldn't it work for everyone else too?

COMPROMISING VIA CI/CD



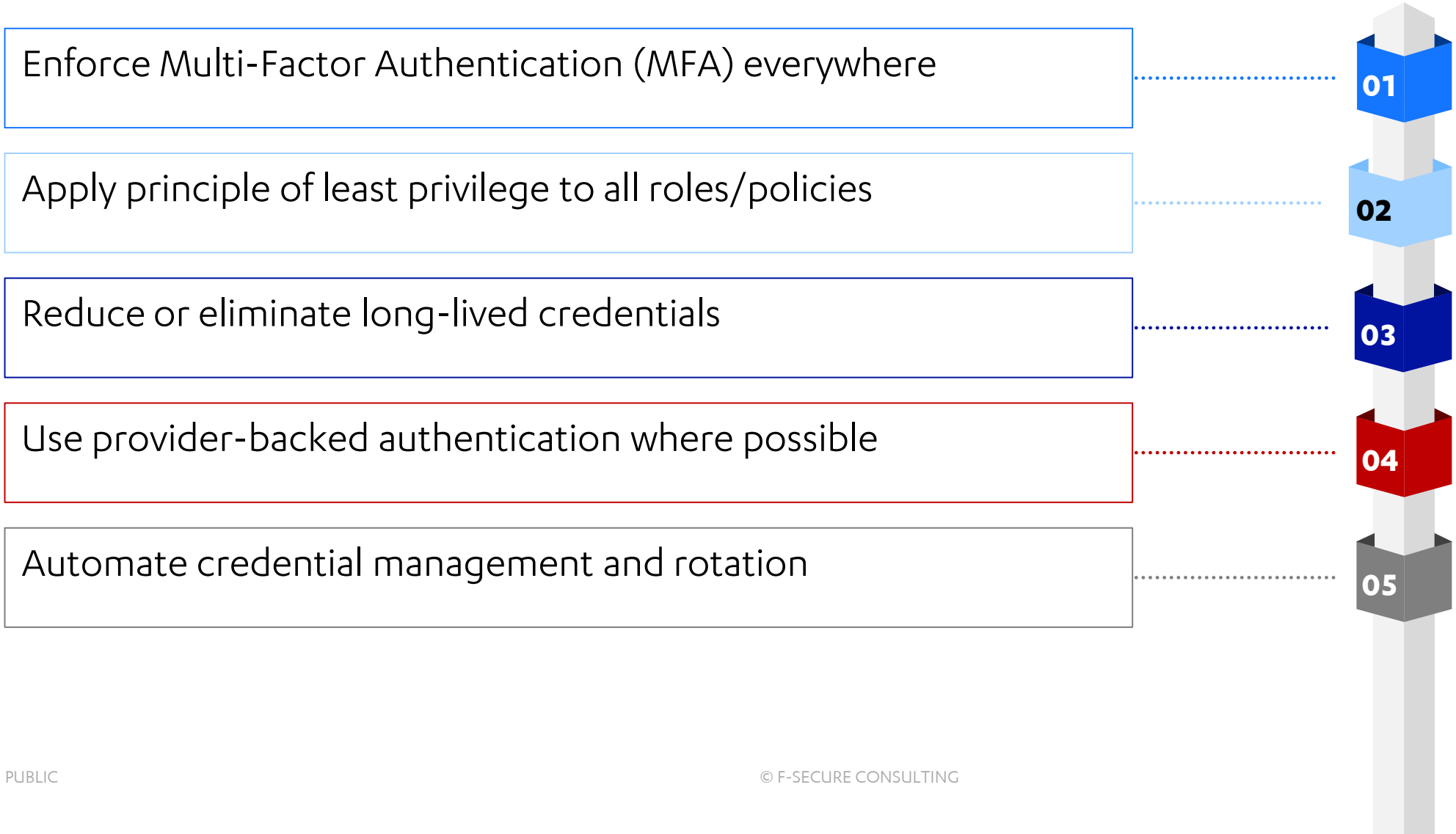
F-Secure

VECTORS WE'VE SEEN EXPLOITED

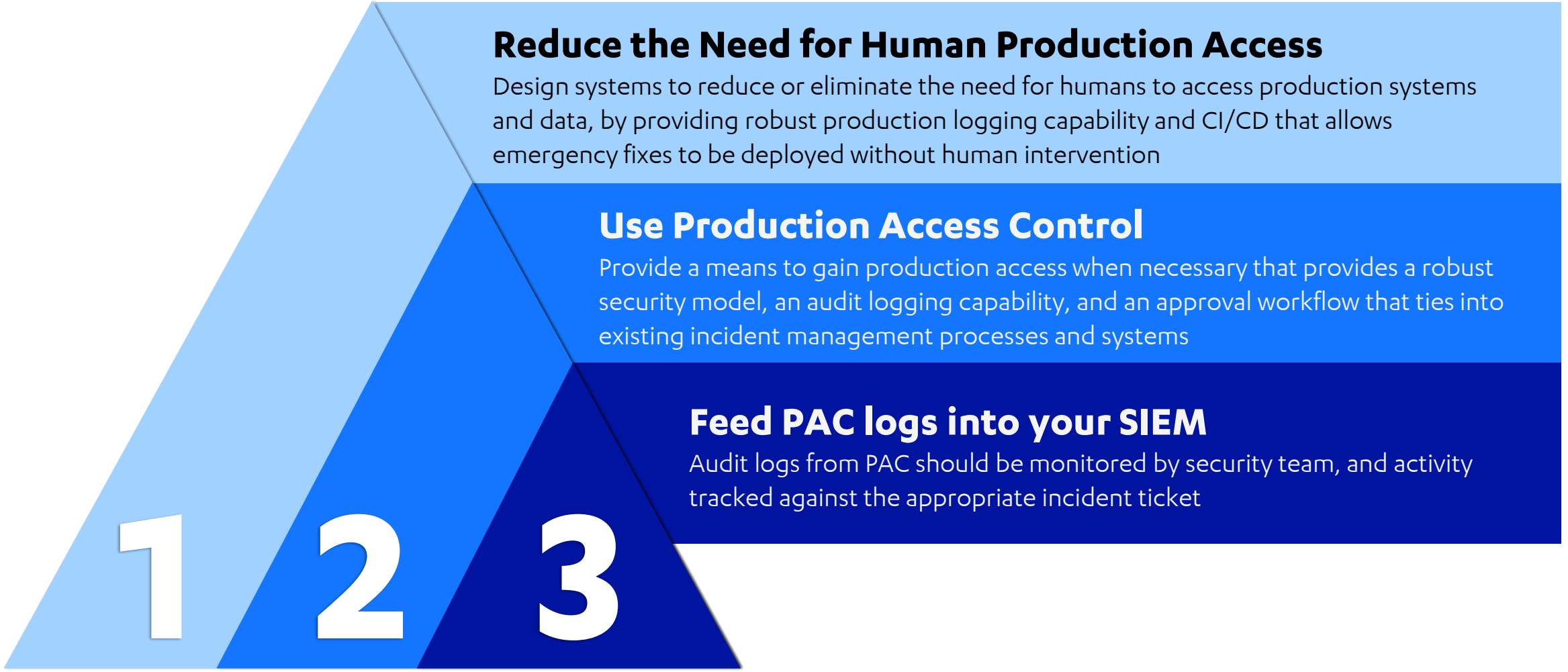


KEY SECURITY CONTROLS

STRONG IDENTITY CONTROLS



AVOID PEOPLE IN PRODUCTION



Reduce the Need for Human Production Access

Design systems to reduce or eliminate the need for humans to access production systems and data, by providing robust production logging capability and CI/CD that allows emergency fixes to be deployed without human intervention

Use Production Access Control

Provide a means to gain production access when necessary that provides a robust security model, an audit logging capability, and an approval workflow that ties into existing incident management processes and systems

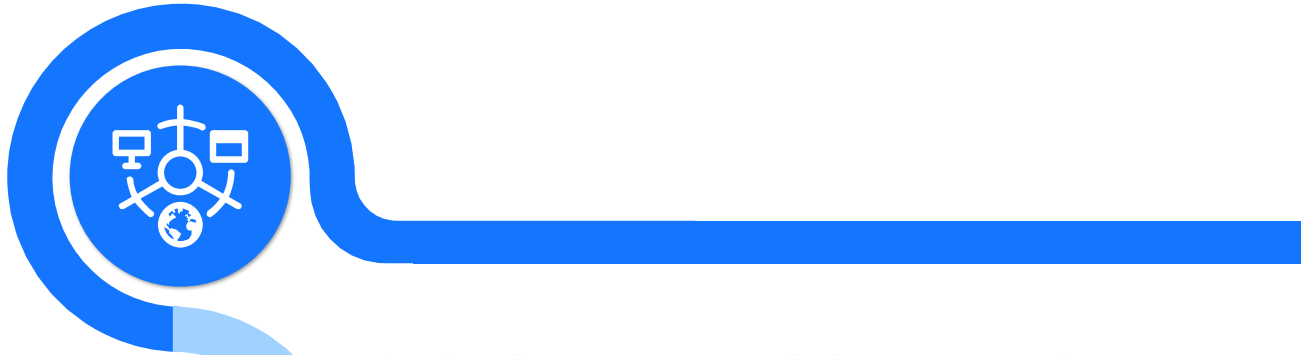
Feed PAC logs into your SIEM

Audit logs from PAC should be monitored by security team, and activity tracked against the appropriate incident ticket

LIMIT BLAST RADIUS

SEPARATE PROJECTS

Use separate accounts/subscriptions/ projects for different applications



SEGREGATE AT THE NETWORK LEVEL

Enforce strong network boundary controls, avoid VPC peering (especially with third parties)

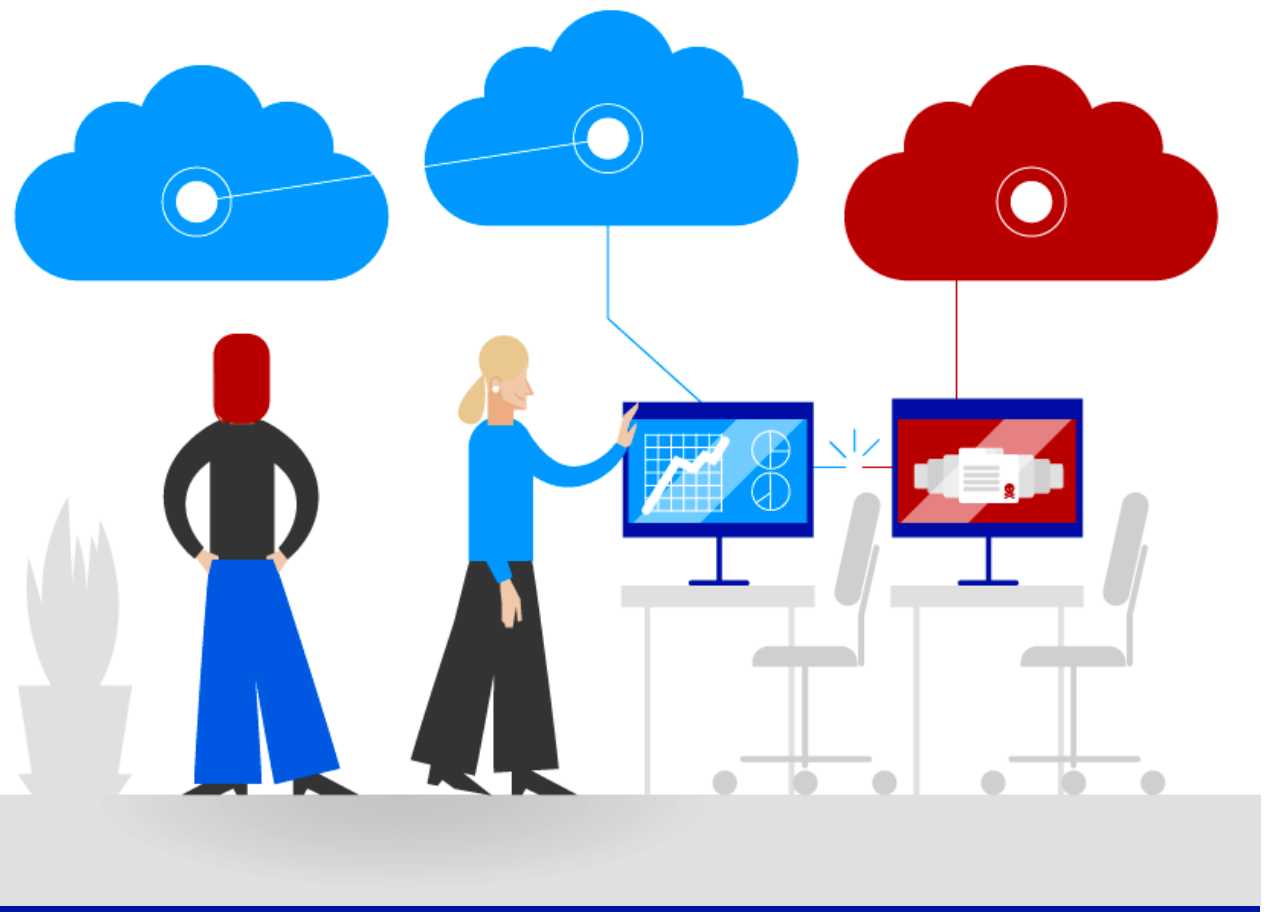
SEPARATE ENVIRONMENTS

Keep development, QA/test and production environments separated within your cloud's management structure, such as AWS Organisations or Google Organisations

MINIMISE SHARED SERVICE ACCESS

Deploy unique CI/CD pipelines per environment, have monitoring tools reach into the account rather than the accounts writing data out elsewhere

SECRETS MANAGEMENT



One of the key failings in most cloud environments

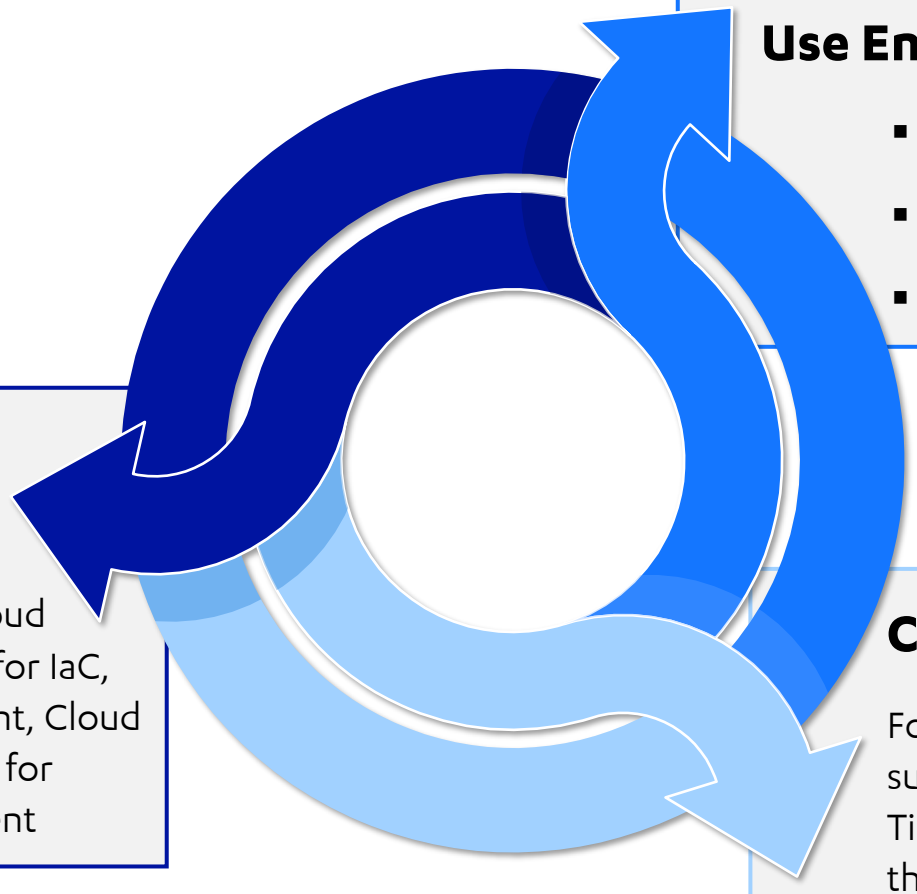
Consider:

- Where applications store their secrets
- How credentials are shared between systems
- How secrets are rotated
- How to identify when secrets are leaked – scanners in CI/CD systems, monitoring internal file shares and knowledge bases

SCALING CLOUD SECURITY

F-Secure

CENTRALISED MANAGEMENT



Use Enterprise Management Features

- AWS Organisations
- Azure Enterprise Enrollment
- GCP Organisations

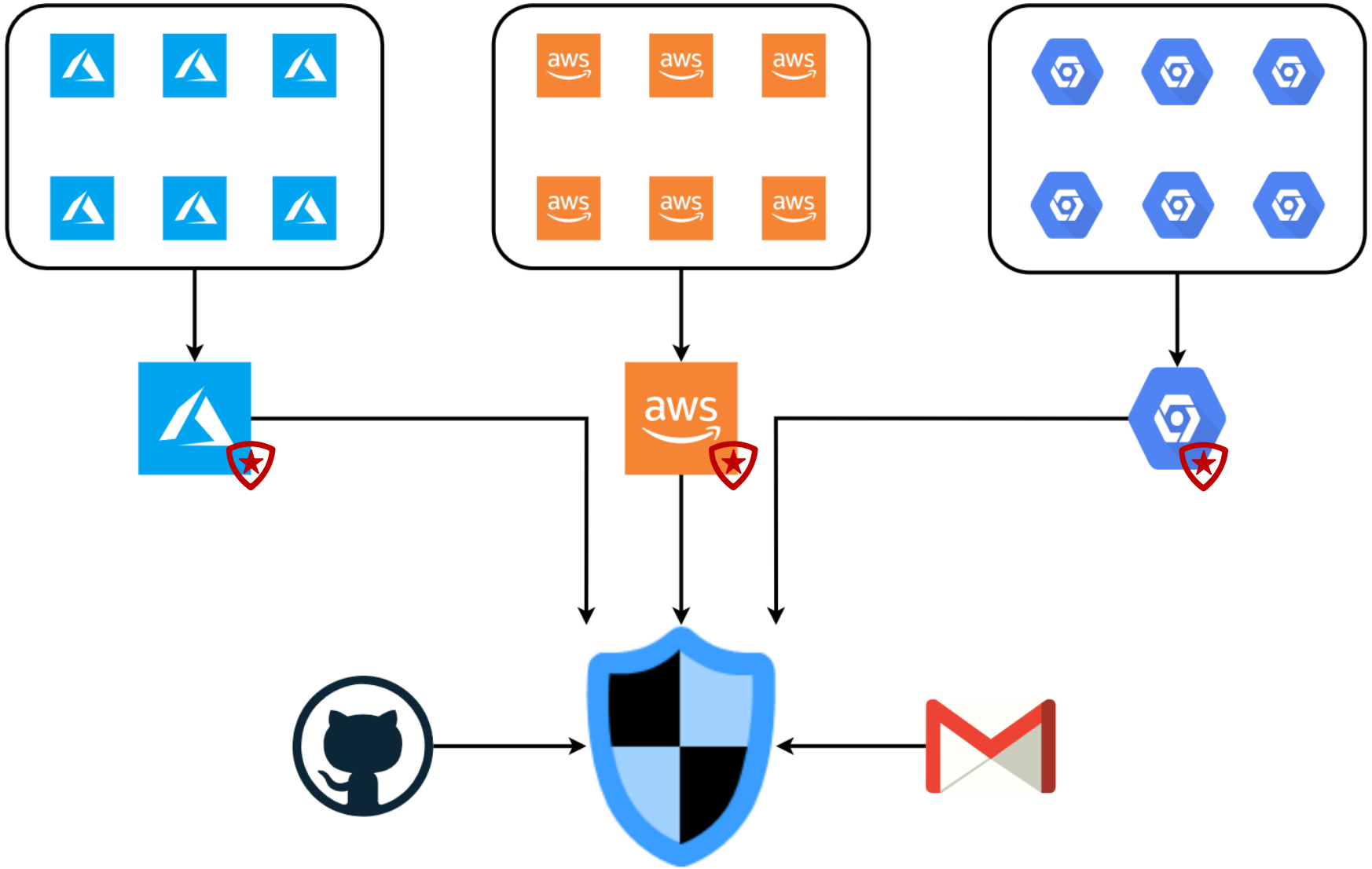
Use Provider-Agnostic Tooling

Pick tools that work across all the cloud providers you work with. Terraform for IaC, Vault/Conjur for secrets management, Cloud Custodian or commercial equivalent for configuration review and enforcement

Centralise Security Functions

For each provider, maintain a security account, subscription or project, and another for logs. Tightly restrict access to these accounts to only those users and systems who really need access

CENTRALISED MONITORING



F-Secure

CENTRALISED MONITORING

LOG SOURCE	BENEFIT
Control Plane audit logs (CloudTrail, Audit Log)	**Visibility of administrative actions within a cloud environment**
API Gateway/WAF Logs	Identify malicious requests to applications
Storage access logs (S3, Storage Accounts)	Track access to sensitive information
Network flow logs	Identify anomalous traffic by source and destination, volumes etc
System logs from any VMs	Grants OS-level visibility of potential attacker activity
Endpoint Detection and Response agents in VMs	Detects malicious activity within VMs as with on premise estates
Application logs	Provides app-specific contextual information
Service Specific Logs (Lambda executions, KMS key access etc)	Shows access and usage of specific resources and services, which may help to track lateral movement or actions on objective

DECENTRALISED SECURITY SKILLS

- Too many technologies and skills
- Security and engineers should collaborate
- Expect to invest heavily
- Ex-engineers make great cloud security people

DECENTRALISED SECURITY PROCESSES

Central security teams will not have the bandwidth to secure everything

Train and empower engineering teams

Do their own threat modelling

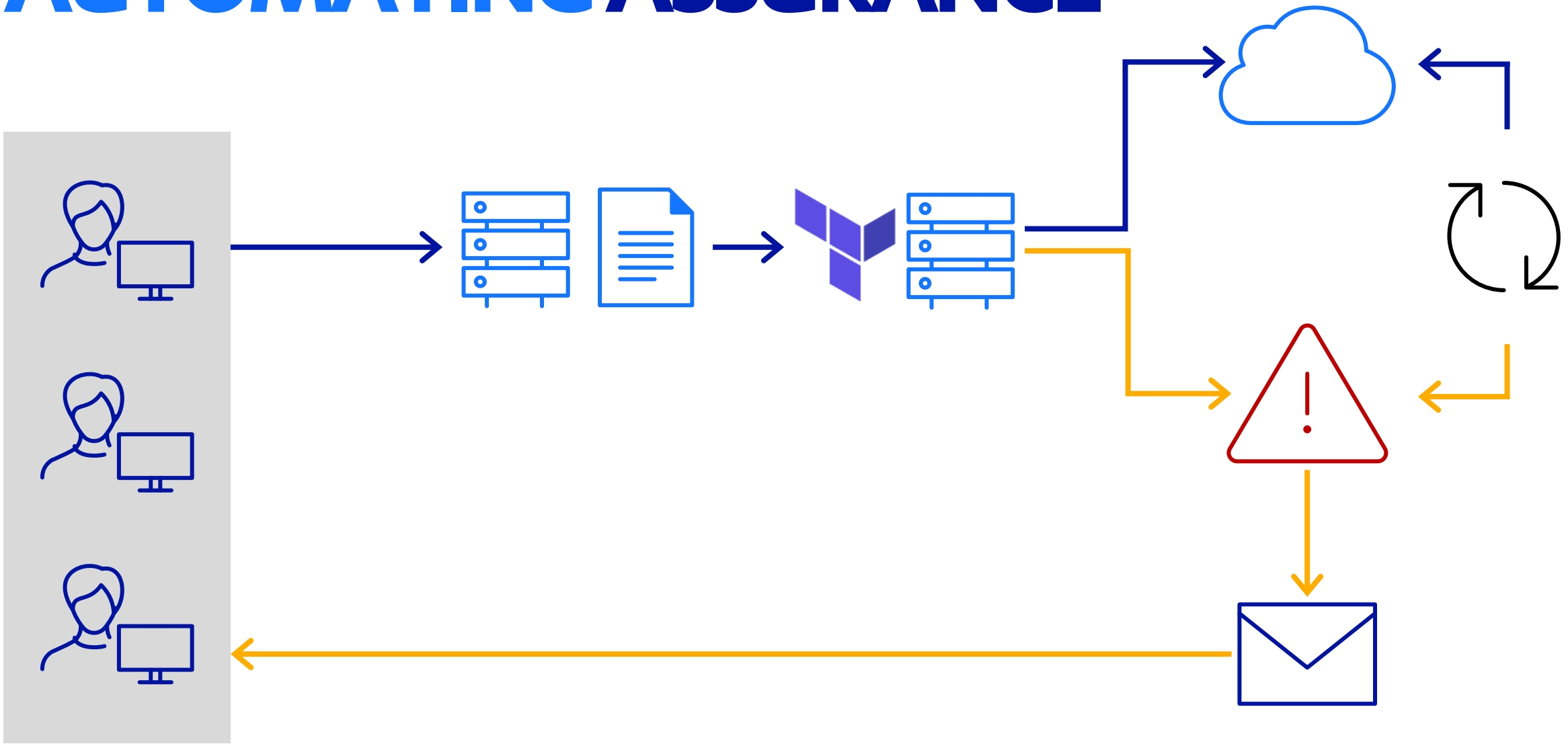
Build and extend relevant security automation

Put security into the engineering process

Cheaper to fix security issues earlier in the process

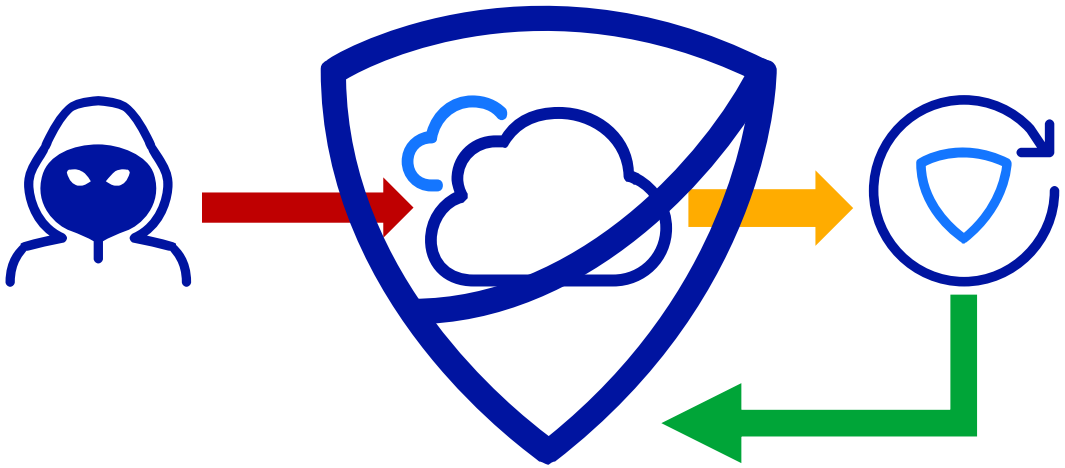
F-Secure

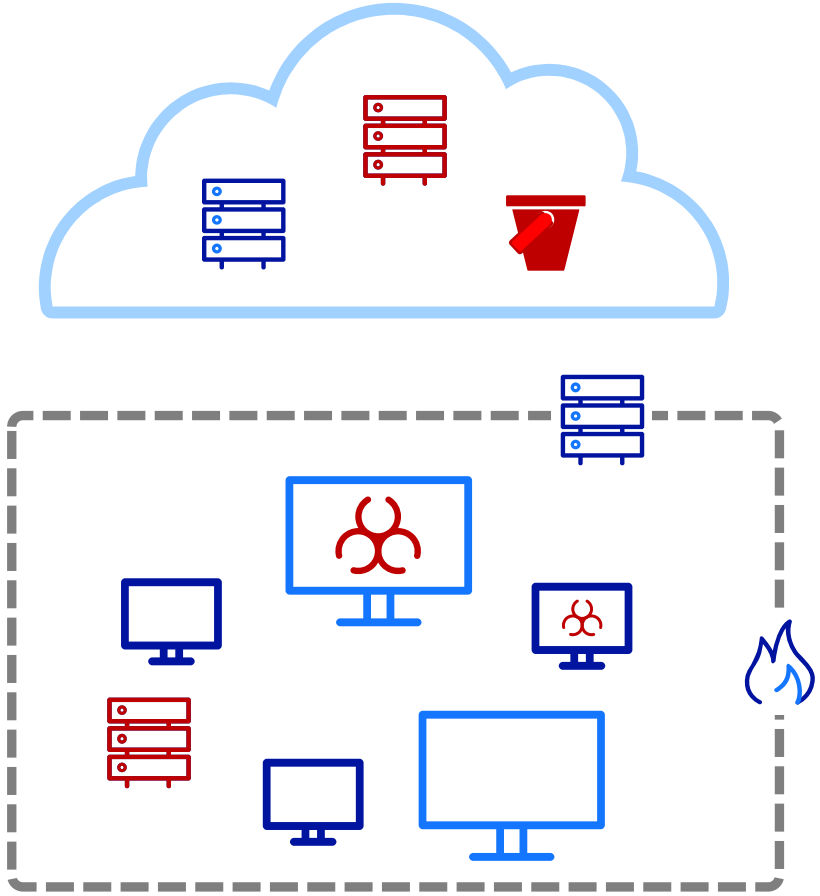
AUTOMATING ASSURANCE



F-Secure

AUTOMATING DETECTION AND IR





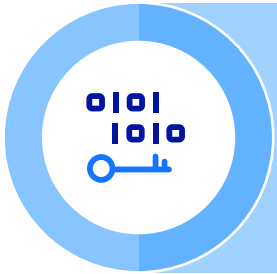
GOAL-DRIVEN TESTING

- Drop compliance pentesting, move to broader, goal-driven assessments
- Testing individual apps in isolation misses the bigger picture
- Test biannually/annually to understand the big picture:
  - External Asset Mapping
  - Attack Detection Capability Assessments
  - Open scope penetration testing / red teaming
  - SDLC pipeline assessments

F-Secure

CONCLUSIONS

Technology changes in the cloud are altering the security landscape



Focus on IAM, secrets management, environment segregation and CI/CD

Leverage automation and empower engineers to scale company-wide

OTHER SLIDES