

How to build secure multi-cloud applications (and still sleep well at night)



Anton Aleksandrov
Chief Architect, IBM Cloud Application Identity

Disclaimer

- **Notice: Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.**
- IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.
- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.
- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.
- The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

None of the statements contained herein constitutes legal advice – it is experience sharing only

Agenda



Anton Aleksandrov
Chief Architect, IBM Cloud Application Identity

- Security breaches
- Security risks and shared responsibility model
- Security your cloud workloads
- DevSecOps
- Network threat protection
- Identity and access
- Data protection
- Gain visibility
- Action items
- Q&A

Cloud is an opportunity to do security right!



“Most breaches occur in North America. It is estimated that the average cost of a data breach will be over \$150 million by 2020, with the global annual cost forecast to be \$2.1 trillion. It is estimated that in first half of 2018 alone, about 4.5 billion records were exposed as a result of data breaches. In 2019, a collection of 2.7 billion identity records, consisting of 774 million unique email addresses and 21 million unique passwords, was posted on the web for sale.”

- Wikipedia

New York (CNN Business) – In one of the biggest data breaches ever, a hacker gained access to more than 100 million Capital One customers' accounts and credit card applications earlier this year.

New York (CNN Business) – Credit reporting agency Equifax has reached a deal to pay up to \$700 million to state and federal regulators to settle probes stemming from a data breach that exposed the personal information of nearly 150 million people. It will be the largest settlement ever paid for a data breach.

London (CNN Business) – British Airways faces a record \$230 million fine after a website failure compromised the personal details of roughly 500,000 customers.

Your company name here ???

Entity ↕	Year ▼	Records ↕	Organization type ↕	Method ↕
Amazon Japan G.K.	2019	unknown	web	accidentally published
2019 Bulgarian revenue agency hack	2019	over 5,000,000	government	hacked
Canva	2019	140,000,000	web	hacked
Capital One	2019	106,000,000	financial	hacked
Desjardins	2019	2,900,000	financial	inside job
DoorDash	2019	4,900,000	web	hacked
Facebook	2019	540,000,000	social network	poor security
Facebook	2019	1,500,000	social network	accidentally uploaded
First American Corporation	2019	885,000,000	financial service company	poor security
Health Sciences Authority (Singapore)	2019	808,000	healthcare	poor security
Justdial	2019	100,000,000	local search	unprotected api
Ministry of Health (Singapore)	2019	14,200	healthcare	poor security/inside job
Mobile TeleSystems (MTS)	2019	100,000,000	telecommunications	misconfiguration/poor security
Quest Diagnostics	2019	11,900,000	Clinical Laboratory	poor security
StockX	2019	6,800,000	retail	hacked
Truecaller	2019	299,055,000	Telephone directory	unknown
Universiti Teknologi MARA	2019	1,164,540	academic	hacked
Woodruff Arts Center	2019	unknown	arts group	poor security
Zynga	2019	218,000,000	social network	hacked
Westpac	2019	98,000	financial	hacked
Australian National University	2019	19 years of data	academic	hacked

AerServ (subsidiary of InMobi)	2018	75,000	advertising	hacked	[13]
Air Canada	2018	20,000	transport	hacked	[15]
Bell Canada	2018	100,000	telecoms	hacked	[44]
Bethesda Game Studios	2018		gaming	accidentally published	[46]
Blank Media Games	2018	7,633,234	gaming	hacked	[47][48]
BMO and Simplii	2018	90,000	banking	poor security	[52]
British Airways	2018	380,000	transport	hacked	[53][54]
Cathay Pacific Airways	2018	9,400,000	transport	hacked	[65]
Centers for Medicare & Medicaid Services	2018	75,000	healthcare	hacked	[80]
Earl Enterprises (Buca di Beppo, Earl of Sandwich, Planet Hollywood, Chicken Guy, Mixology, Tequila Taqueria)	2018-2019	2,000,000	restaurant	hacked	[101]
Facebook	2018	50,000,000	social network	poor security	[118][119][120][121][122][123]
Google Plus	2018	500,000	social network	poor security	[137][138][139]
HauteLook	2018	28,517,244	retail	hacked	[149][150][151]
Marriott International	2018	500,000,000	hotel	hacked	[190][191]
MyHeritage	2018	92,283,889	genealogy	unknown	[204]
Orbitz	2018	880,000	web	hacked	[222]
Popsugar	2018	123,857	fashion	hacked	[225]
Quora	2018	100,000,000	Question & Answer	hacked	[228]
Reddit	2018	unknown	web	hacked	[232][233]
SingHealth	2018	1,500,000	government, database	hacked	[243]
Ticketfly (subsidiary of Eventbrite)	2018	26,151,608	ticket distribution	hacked	[275]
Typeform	2018	unknown	tech	poor security	[65]
Under Armour	2018	150,000,000	Consumer Goods	hacked	[297]
United States Postal Service	2018	60,000,000	government	poor security	[302]
WordPress	2018			hacked	[320]

Factors increasing exposure to security risks



Greater attack surface area from more public APIs, moving to the cloud, and increasing third-party integrations



Stronger and more sophisticated attackers



Greater scrutiny by government and media around data, privacy and security

Shared Responsibility Model

The cloud provider is responsible for Security **Of The Cloud** (for which it takes responsibility).

The customer is responsible for Security **In The Cloud**.

Securing your Cloud Workloads



Information
systems

Network

Protection

Internet
attack

Cyber
security

Hacker

Internet

Mobile
devices

Computer

Cloud is an opportunity to do security right



Developers

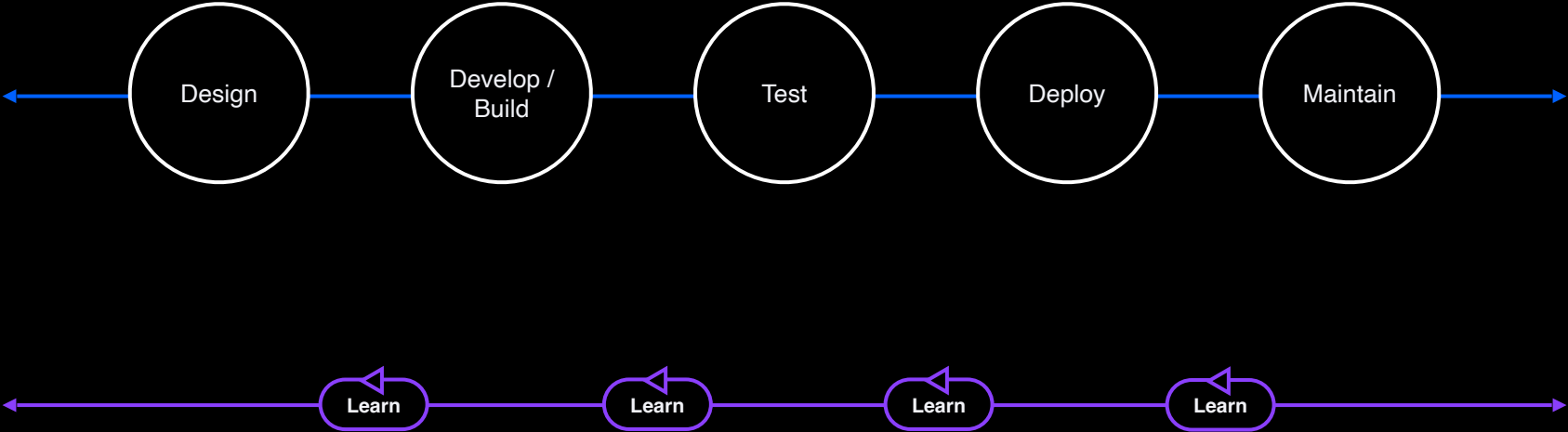


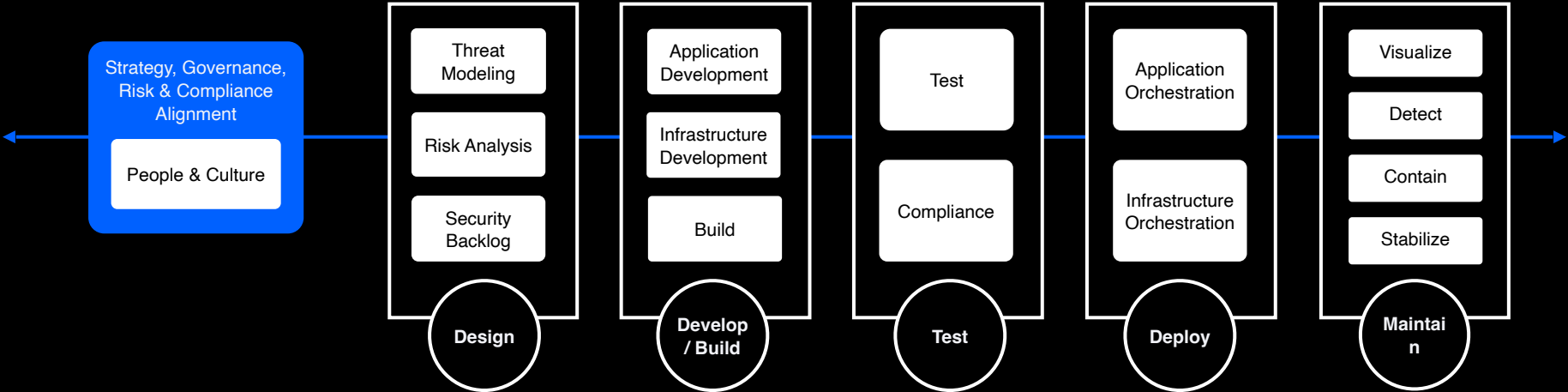
Security

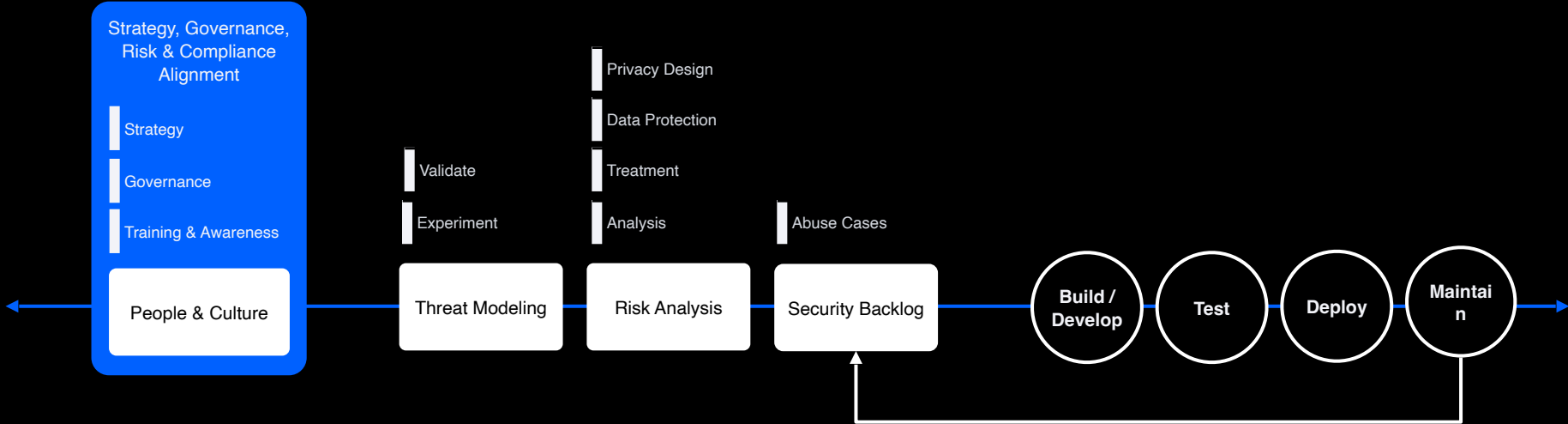


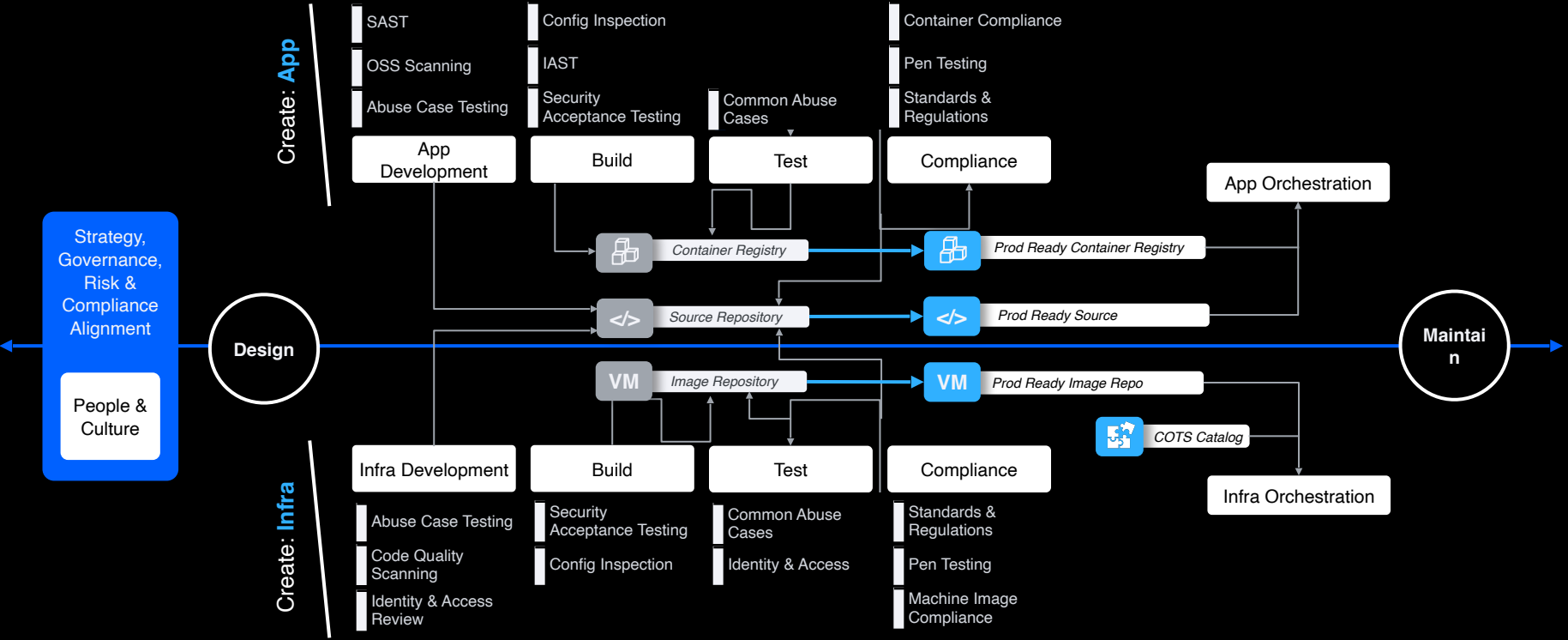
Management
& Operations

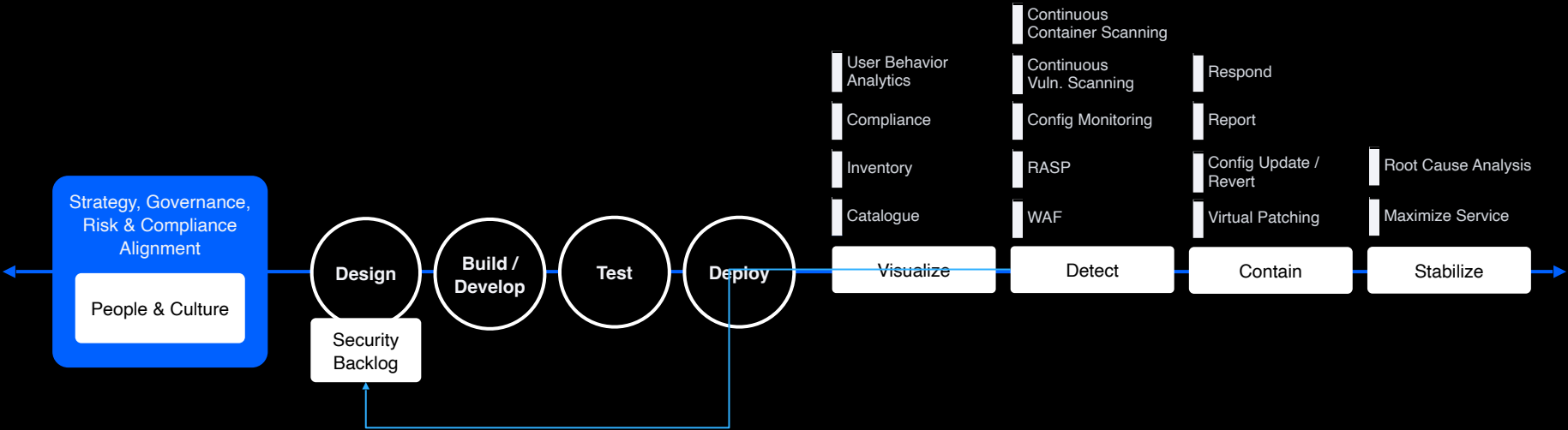
DevSecOps



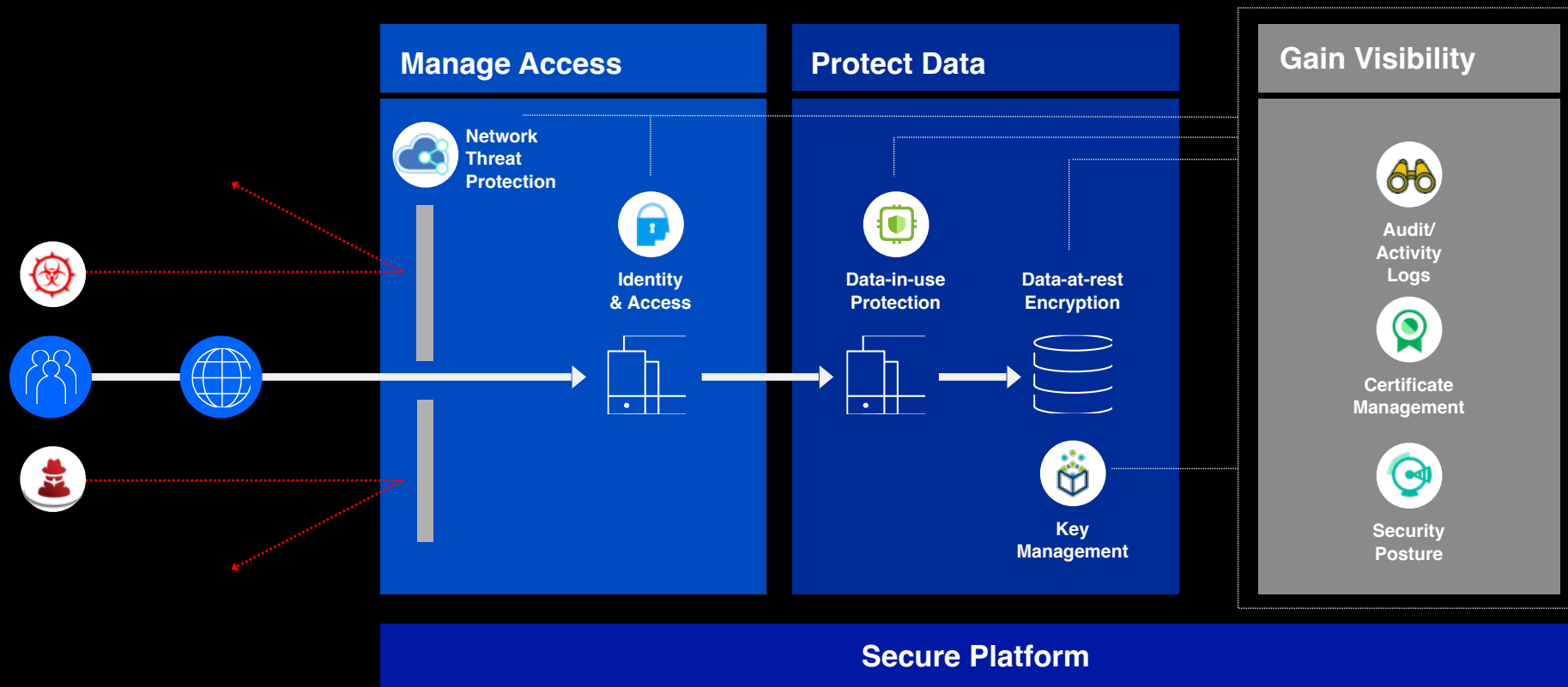




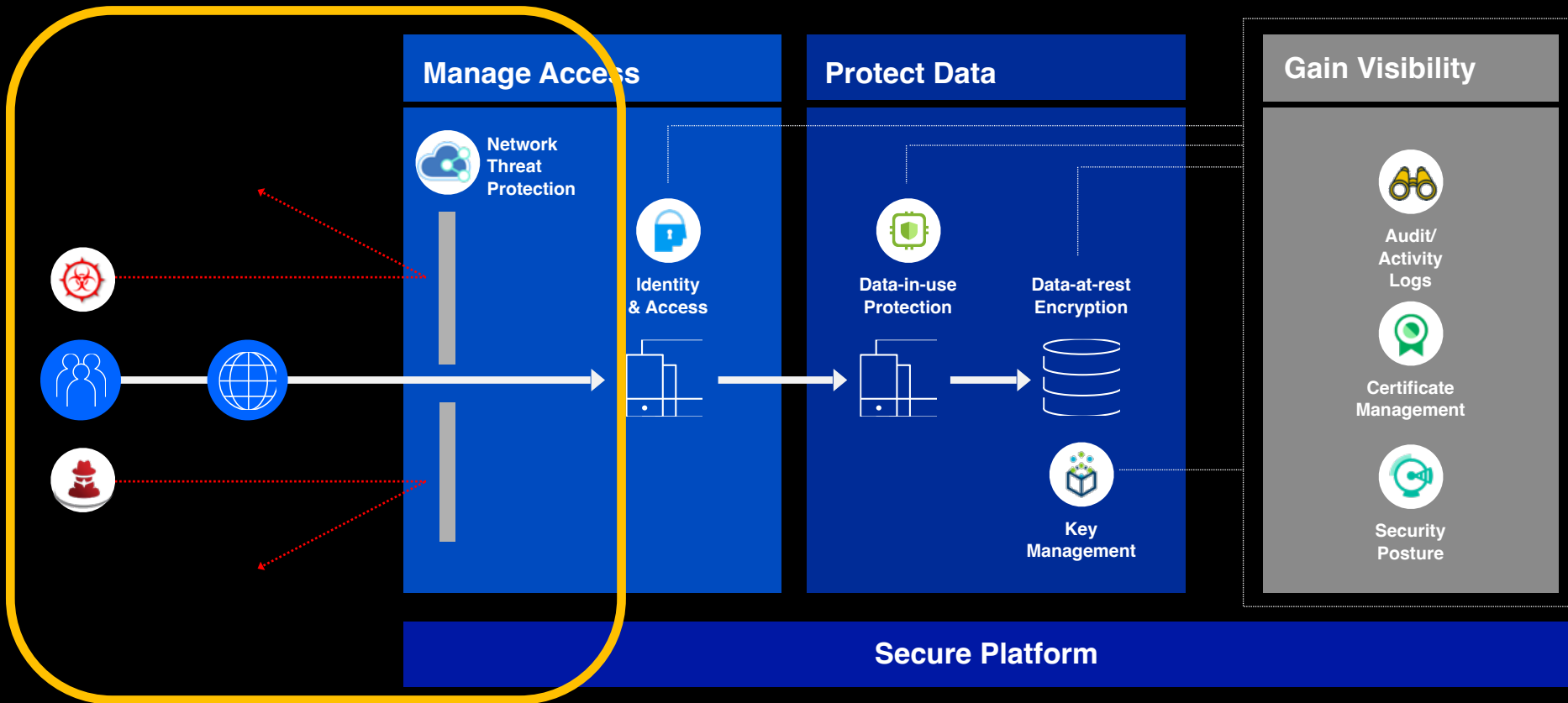




Achieving continuous security involves an end-to-end solution











Achieving continuous security involves an end-to-end solution



Network Threat Protection

Using classic Firewalls is no longer good enough...

<div>SECURITY</div> <div></div>	<ul style="list-style-type: none">• DDoS Protection: Protect against volumetric, Layer 3 & 4 and application attacks at Layer 7• Web Application Firewall (WAF)/IP Firewall: Protect applications and websites against both known and new exploits• Transport Layer Security(TLS): Ensure secure data transfers using the latest encryption standards• Rate Limiting: Protect applications and websites against volumetric application and brute force attacks
<div>RELIABILITY</div> <div></div>	<ul style="list-style-type: none">• Domain Name Server (DNS): Fast resolution of hostnames to their corresponding IP addresses or aliases.• Global Load Balancer (GLB): Increase availability by routing traffic across servers based on their availability and service health.
<div>PERFORMANCE</div> <div></div>	<ul style="list-style-type: none">• Caching: Provide visitors with location-based access, removing latency and improving performance• Page Rules: Manage granular actions on a web page, create redirects, or fine tuning caching behavior• Smart Routing: Ensure content is delivered on the fastest path from end user to application, website or API

Network Threat Protection

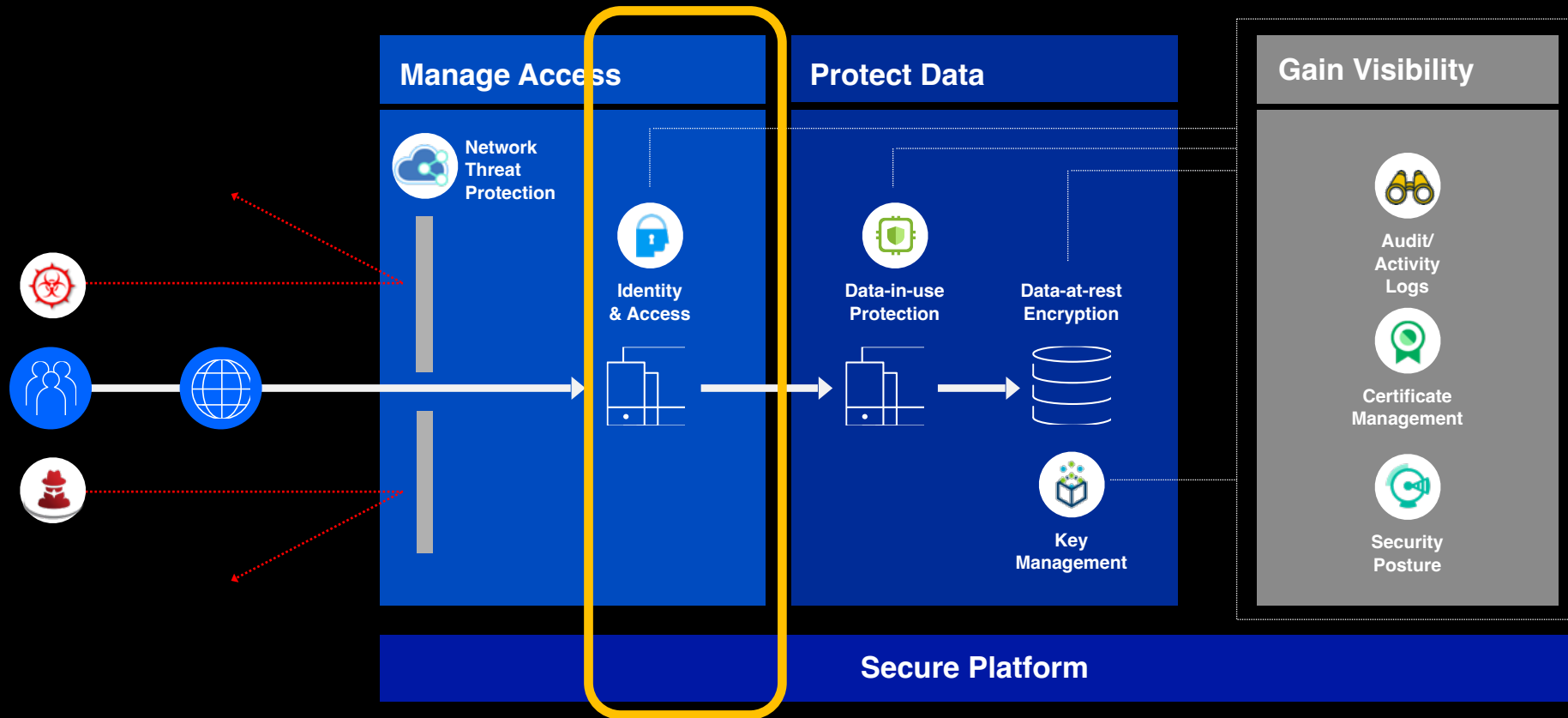
Without Network Threat Protection



With Network Threat Protection



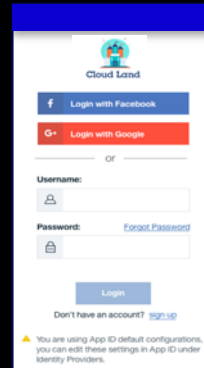
Achieving continuous security involves an end-to-end solution



Identity solution for application developers



Add authentication to your mobile and web apps and protect your APIs and back-ends running on cloud. Add email/password based sign-up and sign-in, or social log-in. For employee-facing apps, use SAML 2.0 federation for enterprise sign-in. For all app users, enrich their profiles with additional info so you can build engaging experiences.



Authentication / Authorization

- Email/Password, Social sign-in, Enterprise sign-in
- Open sourced Server and Client SDKs for most popular programming languages
- Secure your apps running on Kubernetes or your managed APIs with no code changes
- Open standards based (OAUTH2, OIDC, SCIM, SAML 2.0)

24



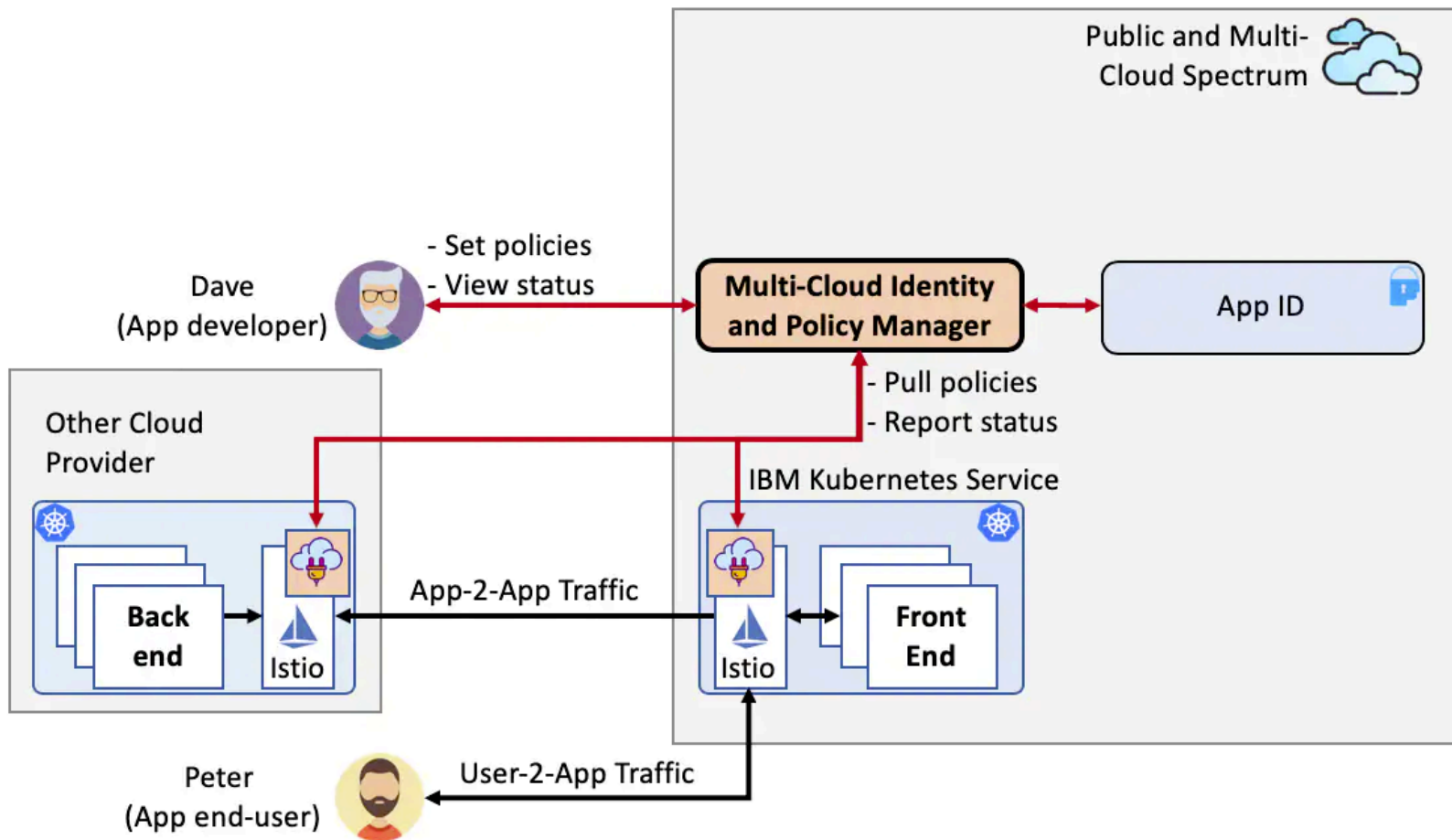
User Management

- Sign-in, sign-up, email verification, change password, forgot password
- Default UI and flows, or replace with your own branding and custom flows
- Default email templates you can customize and brand

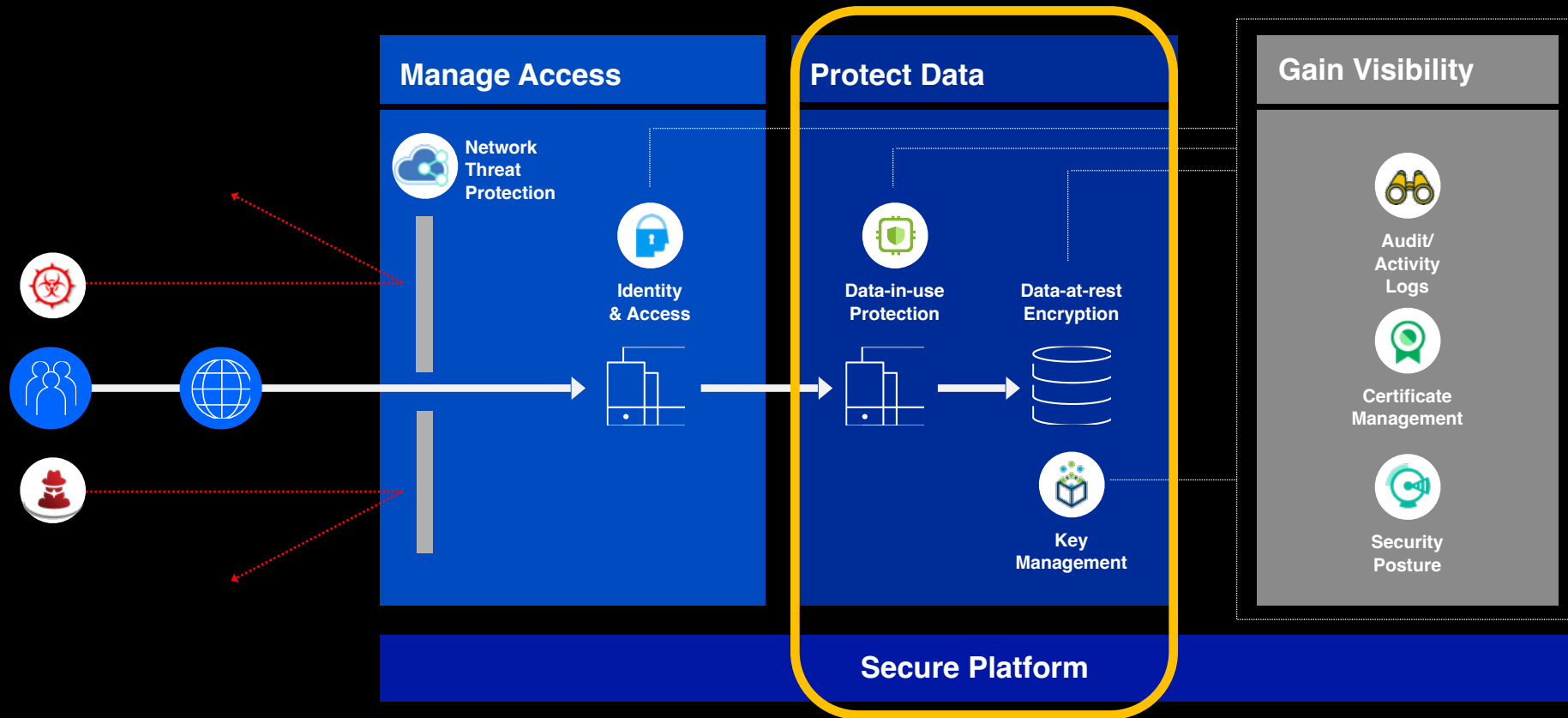


Application User Profile Management

- Store end user data, like app preferences, to personalize app experiences
- Leverage data from user repositories, or add your own custom attributes
- Continuity for users who start out anonymously and sign-in later



Achieving continuous security involves an end-to-end solution

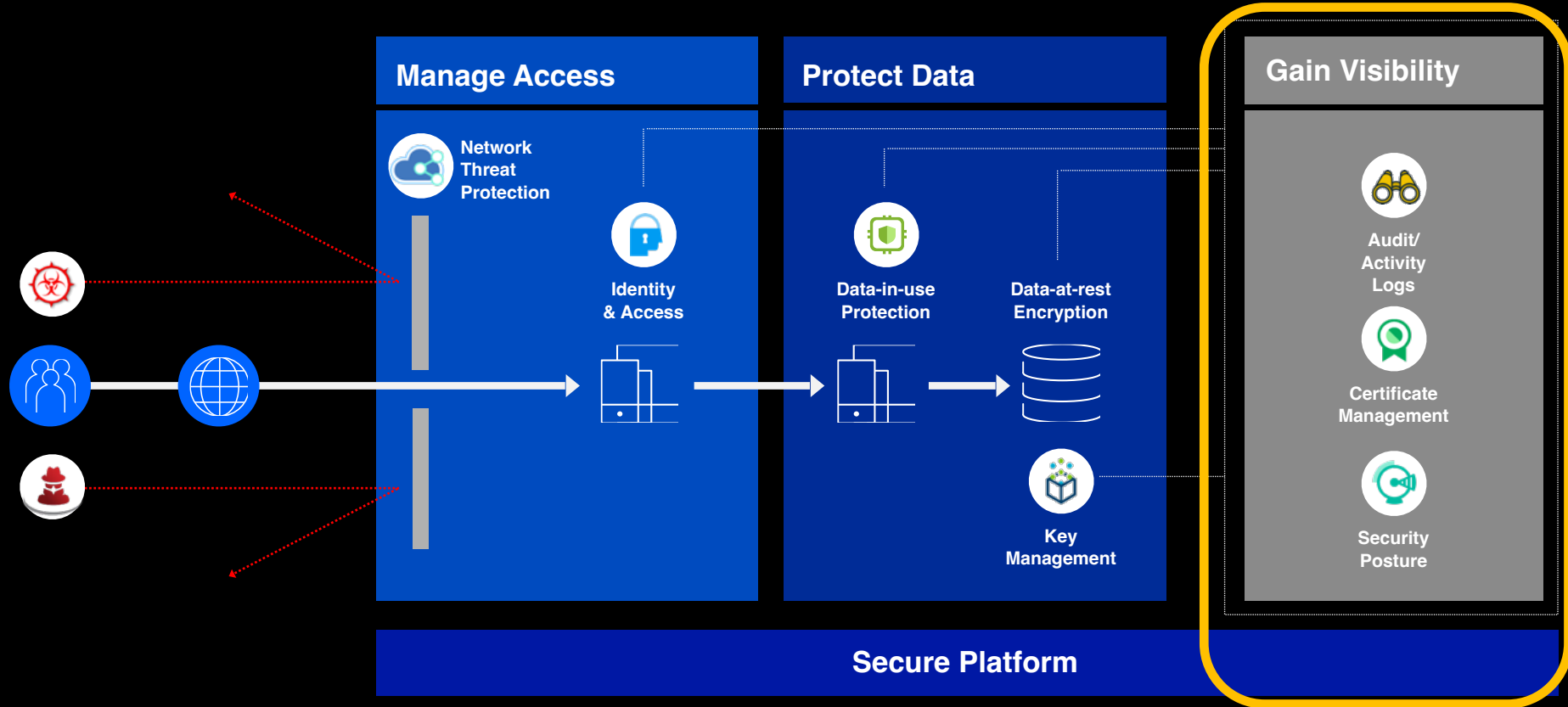


Securely storing data

- Only use storage types that support data encryption
- Use Cloud key management services for the keys that YOU OWN
- Pick an HSM based key management service
- Data-at-rest encryption using BYOK/KYOK
- Runtime Encryption using Data Shield and application encryption
- Prevent Cloud providers or any third party from being able to access your data



Achieving continuous security involves an end-to-end solution



Audit / Activity Logs

Actively track Cloud activities for security, audit, and debug


- **Record developer actions** such as cloud resource access, configuration changes etc.
- **Record user actions** such as authentication success/failure, action performed etc.
- **Alert into action** with multi-channel notification support through Pager Duty, Slack, webhooks etc.
- Find and fix issues faster with **intuitive search query** and lightning fast search.
- **Download event data** for ad hoc analysis
- **Data is stored as CADF** for compliance for audit, insight, and cross vendor compatibility

Hosted to scale with your mission critical applications


- **Automated Archive** to Cloud Storage
- **Compliance:** GDPR, Privacy Shield, PCI, SOC2, HIPAA etc


Audit / Activity Logs

← → ↻ 🔒 https://app.us-south.logging.cloud.ibm.com/c0182c47eb/logs/view/73d4781c6a?b=1... ☆ 🖨️ 📄 🔄 🌐 📱 🏠





Find a View

 DASHBOARD

 EVERYTHING

VIEWS

 DEMO VIEWS


 SECURITY


All Activities


Bucket operations

Cert lifecycle

CF events

 TEAM OPS





All Activities ▾ randys-mbp ▾ All Apps ▾ All Levels ▾

Nov 9 16:06:26 randys-mbp at.log Push Notifications: create key Johnny-cred
Nov 9 16:09:08 randys-mbp at.log Key Protect: create secrets
Nov 9 16:10:30 randys-mbp at.log Cloud Foundry: update app KeyProtectTest
Nov 9 16:11:49 randys-mbp at.log IAM Identity Service: login user-apikey KeyProtectTest
Nov 9 16:11:49 randys-mbp at.log Key Protect: delete secrets
Nov 9 16:11:49 randys-mbp at.log Cloud Foundry: update app KeyProtectTest
Nov 9 16:13:12 randys-mbp at.log Key Protect: list secrets Key Protect-se
Nov 9 16:13:12 randys-mbp at.log Key Protect: list secrets Key Protect-se
Nov 9 16:13:12 randys-mbp at.log Key Protect: list secrets Key Protect-se
Nov 9 16:14:34 randys-mbp at.log Cloud Foundry: update service_instance Log Analysis-legacy

View in context ⓘ Copy to clipboard 📄 Share this line ➦ Close ✕

@timestamp 2018-11-09T21:09:53.642Z

@version 1

action audit.service_instance.update

ALCH_ACCOUNT_ID (empty)

ALCH_TENANT_ID acf50c90-02d3-4bb5-b402-61ee03dfa7ec

eventTime 2018-11-09 21:09:46.260472 +0000 UTC

event_uuid 28e90bbc-51d2-46bb-90c5-17013ef79f8f

id ba6814c5-1b91-4a14-aecc-db63da93abba

initiator

name rbertram@us.ibm.com

id 40a74b0f-fa0f-48d0-ba60-fb268218b9c3

logmet_cluster topic3-elasticsearch_3

logSourceCRN
crn:v1:bluemix:public:audit:eu-gb:a/8131c65c6ad70bdc209bb564997a5f1c:8424aeea-ddcf-4dfe-ae90-1a4b89e07b86::

⚙️ 86e0c72c-0787-4867-851d-... IBM-DAY 🔍 Search... ⌚ Jump to timeframe ⌚ 🛠️ ● LIVE

Certificate Management Services for Admins and Developers



Certificate Management helps security admins manage the lifecycle of SSL/TLS Certificates and govern their usage in the Cloud environment, while letting developers with little security knowledge deploy certificates easily and securely for their apps, as part of automated dev-ops processes.



Avoid Outages

- Visibility into which certificates you have and where they are in use
- Proactive notifications on soon to expire certificates (Slack, Callback URL, Security Advisor)
- REST APIs that enable automated flows for renewing and deploying (rotating) certificates



Secure TLS Keys

- Import and securely store 3rd party certificates and associated keys
- Visibility into certificate usage
- Control access to certificates (Cloud IAM)
- Audit certificate/key
- Securely deploy to Kubernetes or API Gateway
- Ensure certificates comply with policy



Easily enable TLS

- Easily deploy certificates for custom domains to Kubernetes or API Gateway
- Use Cert Manager APIs to deploy elsewhere
- Easily order free certificates

Security Posture Services

What it does



By centralizing visibility, providing alerting and enabling drill down to resolution, Security Advisor services empowers the Security Focal to manage security for cloud workloads



Security Risks & Posture

A single place to look for your security status

- Known issues and in container images
- Monitor SSL certificate expiration
- Insecure configurations
- Security vendors integrations



Detect Threats

Detect suspicious network and user activity

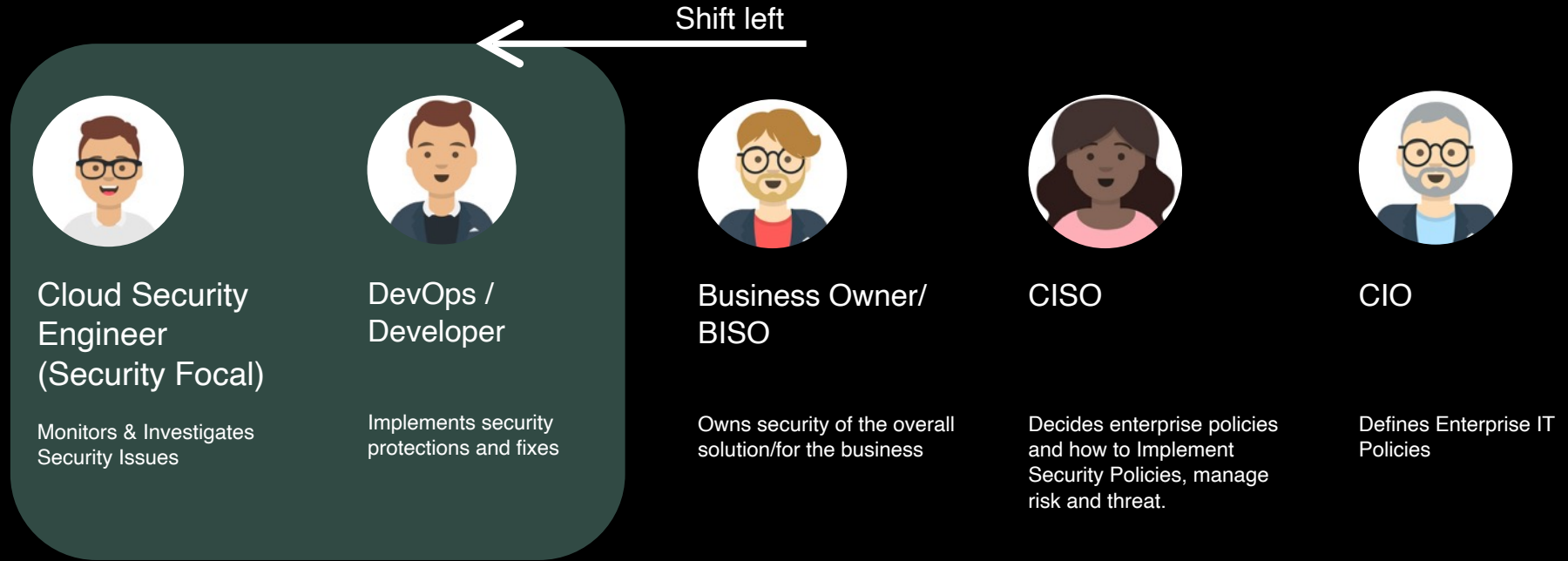
- Communication between your cluster and IPs listed in threat intel sources
- Identify suspicious behavioral changes that reflect malicious activity



Centrally Manage Security

- Plug-in and monitor security issues from various cloud services
- Plug-in findings from your trusted suite of vendors
- Your own “custom integrated” security tools

Who Are the Users?



Others – IT admins, Auditors

Cloud introduces new challenges:

Shift left – developers/devops have new responsibilities, but they're not highly skilled in security, and expect very easy, handy tools

Most classic / legacy security tools today are not a good fit for cloud workloads, not K8 aware, not dev-ops friendly

Cloud requires continued, proactive awareness of changes and new threats:

- Resources come and go
- Deployed workloads change often
- New vulnerabilities discovered



Cloud Security
Engineer
(Security Focal)

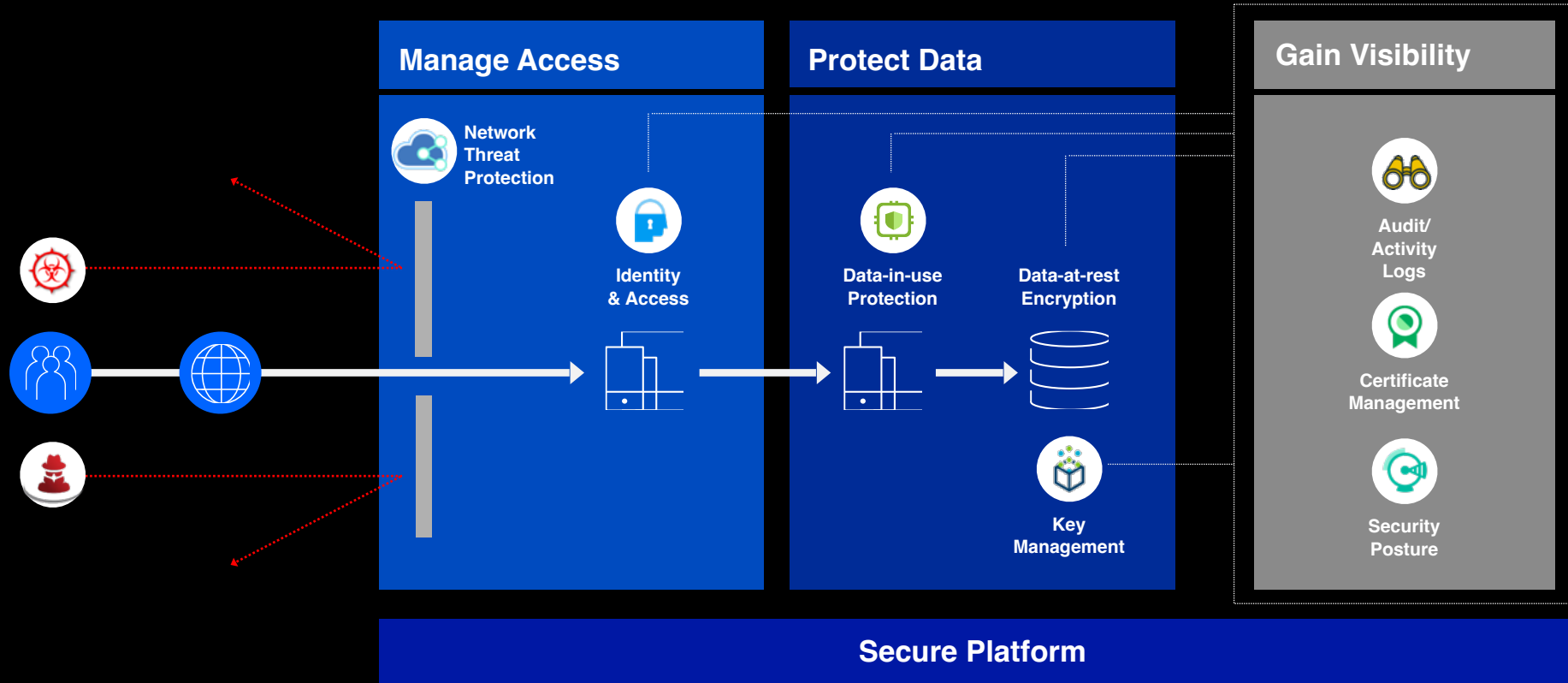
Monitors & Investigates
Security Issues



DevOps /
Developer

Implements security
protections and fixes

Achieving continuous security involves an end-to-end solution



Lets look at some of the activities that should be taken...

Restricting
network
access

Restricting
user
access

Protecting
your Data

DevSecOps
and
Visibility

Restricting Network Access Patterns

Micro segmentation with application centric model

- Segment your μ Services in **Kubernetes** using network policies
- Segment your **Kubernetes** resources using Network/Calico policies

Protecting at the Edge

- DDOS and WAF protection

Legacy firewalls for pure IAAS and VMWare workloads

- Where changes to the workload are slow and limited



Restricting User Access Patterns

Segment Access Using **Platform IAM** Accounts and Resource Groups

- Prod vs. Pre-prod vs. Test vs. Dev account with different user population
- Resource Groups for teams

Use of **Platform IAM** to limit access to platform resources

- Identity Federation, groups and maps
- Limiting access with tight ACLs

Identify users and μ Services in your apps

- User Authentication with **App / User identity service**



Data Protection Patterns

In transit patterns – always use SSL/TLS

- Even inside your Kubernetes cluster
- Use **Certificate Management** service to assure certificates are up-to-date
- Use **Service Mesh**, e.g. Istio, to ensure in-cluster mTLS

At rest pattern: Encrypt your DBs and Buckets

- Bring your own keys with **Key Management Service**



Visibility and Dashboarding

Track all activity in your accounts

- Especially important in the production accounts – easier when access to the account is limited

Visualize your security posture including information coming from:

- Cloud platform tools
- 3rd party security tools
- Home grown tools



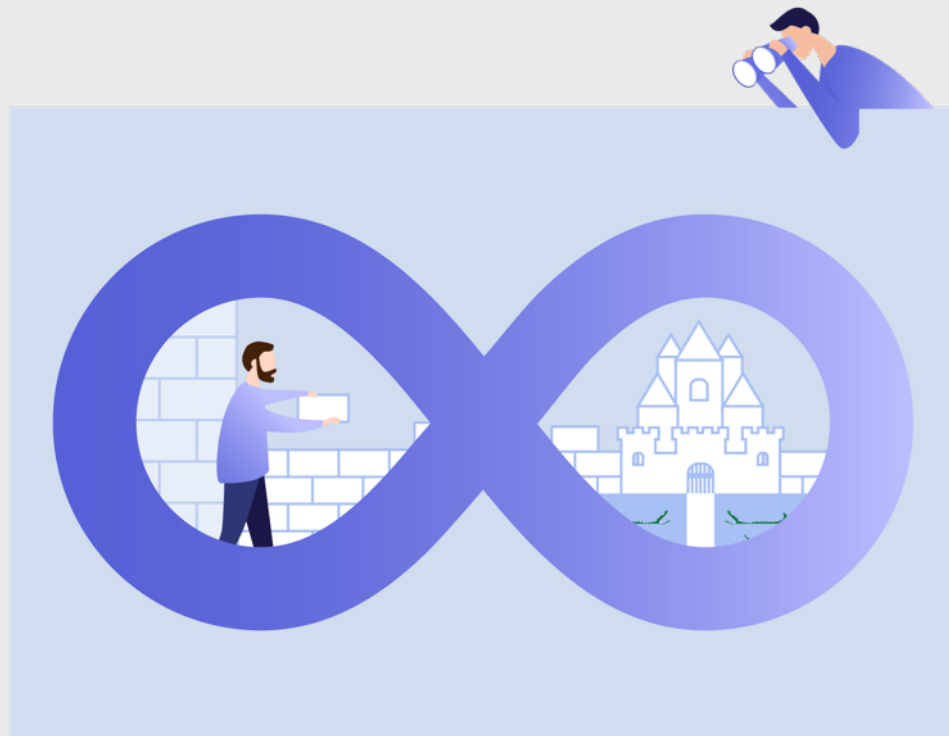
DevSecOps Patterns

Reduce production environment access with certified DevOps flows

- Eliminate direct use of platform cli, kubectl etc. in production. Limit in dev/test.
- Limit user access to the DevSecOps functional user
- Cornerstone of repeatability in DevSecOps

Continuously Scan for vulnerabilities

- Always scan images before deploying and keep track of validity in runtime
- Scan your packages and code before deployment



Thank you