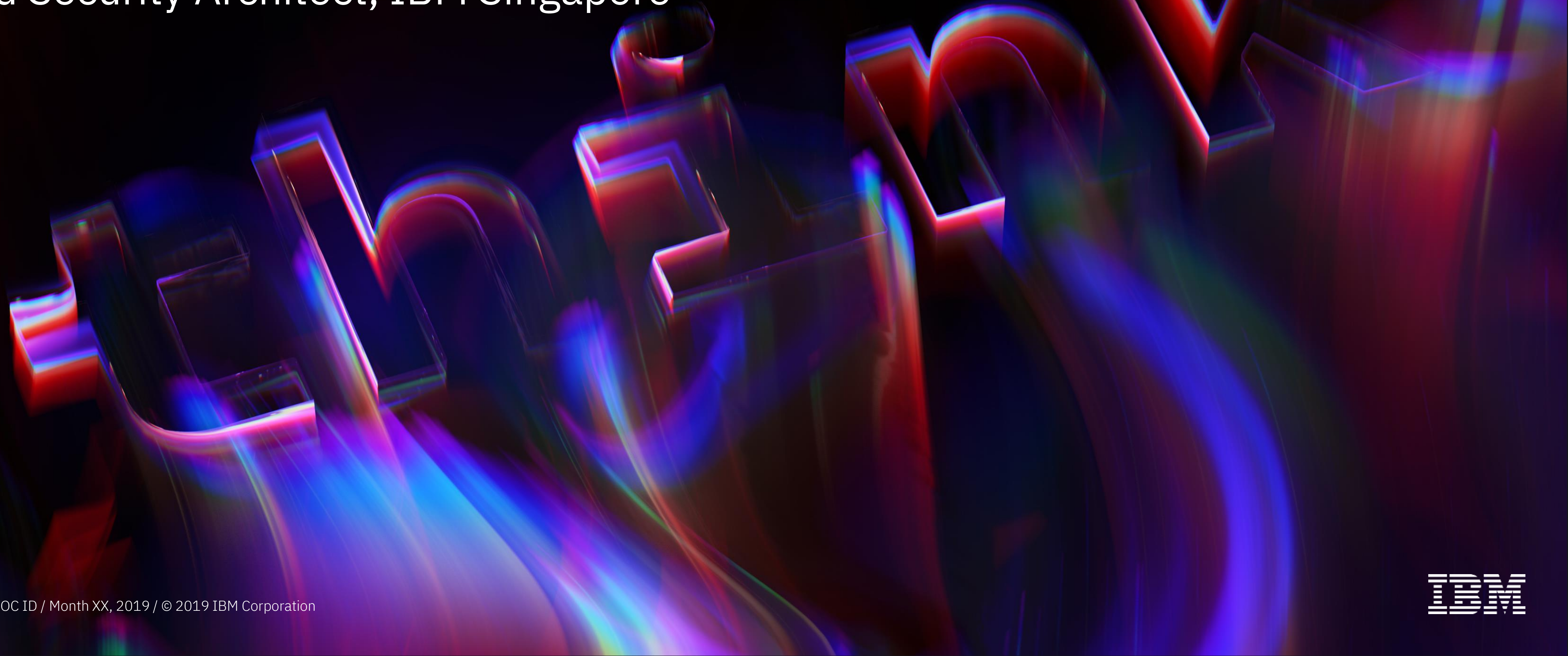
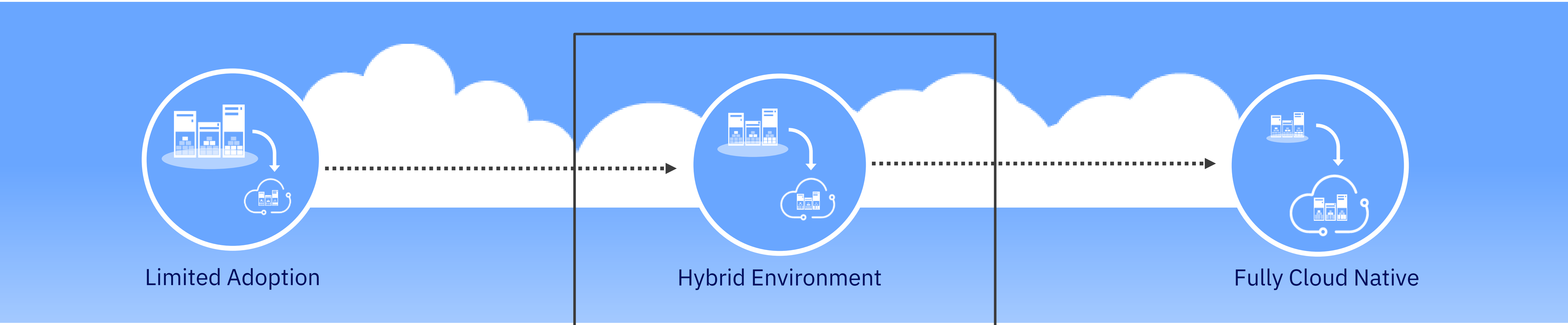
Comprehensive Security to Empower Hybrid/Multi-Cloud Transformation with Confidence

—

Jagadish Paranthaman
Cloud Security Architect, IBM Singapore



Organizations migrate to cloud to get **state-of-the-art IT** in a **cost effective** and **flexible** manner. Their cloud adoption can be broadly mapped to one of three phases



Limited Adoption

Hybrid Environment

Fully Cloud Native

Using some SaaS services and understand that they have Shadow IT issues

Formally starting on Cloud journey, or just starting to move workloads to cloud. Considering deploying workloads to Cloud but unsure how to start.

Well into cloud transformation or primarily in a hybrid steady-state operation

IT organizations with workloads on-premise, but also actively moving workloads to cloud; they understand that they have incomplete controls.

Mature cloud adoption, or born-in-the-cloud organizations

IT organizations born in the cloud and/or using multiple Cloud Services Providers, with extensive DevOps with security considerations.

By 2020, 90% of organizations will adopt hybrid IT infrastructure

Cloud introduces a native set of security controls, unique to each service provider

Hybrid-cloud security is complex.

Cloud Service Provider in the mix now; Infrastructure that’s not yours. CSPs offer their own set of security controls

Need to normalize disparate security controls across hybrid & on-premise environments

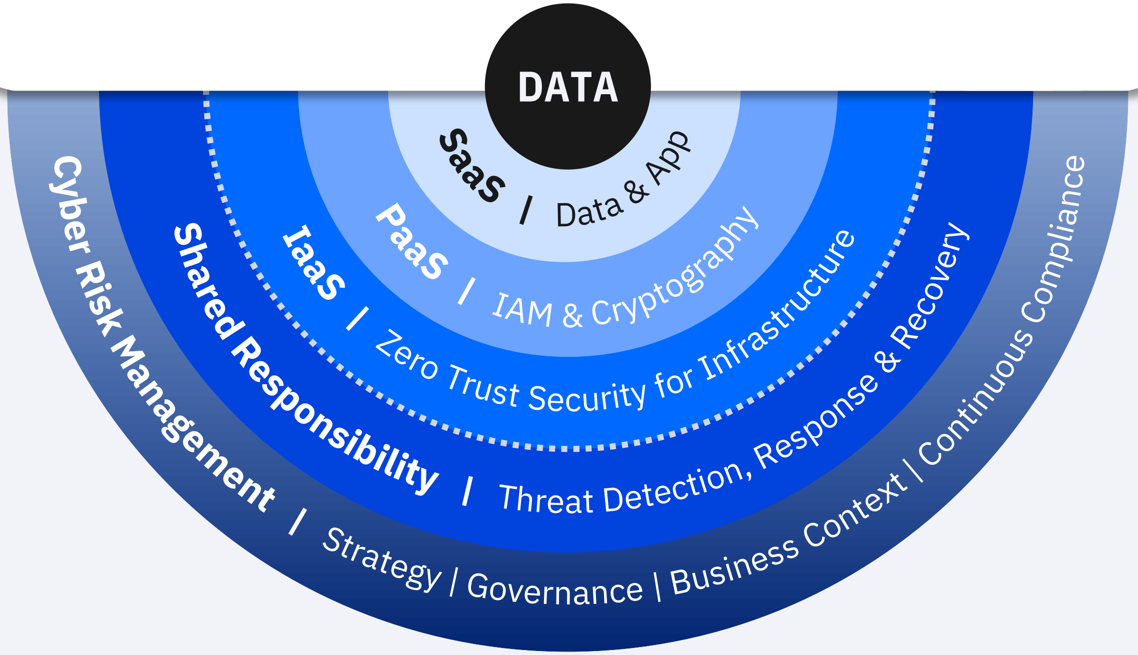
Cloud security talent is hard to find.

Cloud security introduces new skillsets beyond traditional security roles – New tools, new architectures, etc.

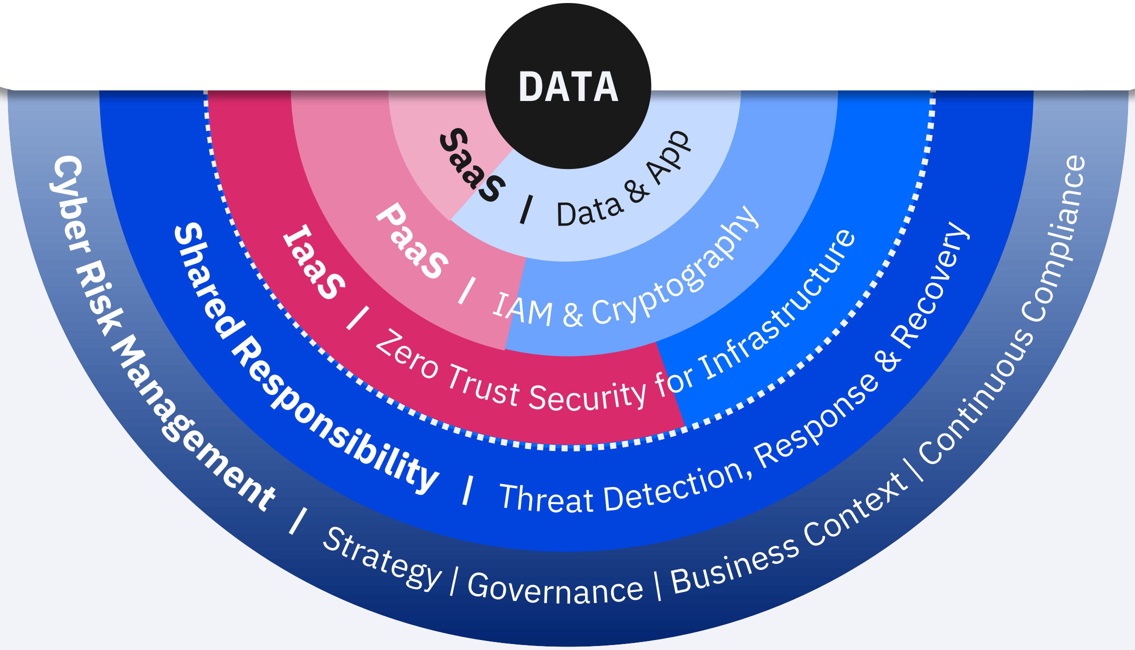
By 2022, there will be 1.8 million unfulfilled cybersecurity jobs

Security can be a **driver** for cloud adoption with the right **framework and programmatic approach**

Securing Enterprise Cloud spans the entire security landscape, with data as the center of the universe.


DATA
SaaS / Data & App
PaaS / IAM & Cryptography
IaaS / Zero Trust Security for Infrastructure
Shared Responsibility / Threat Detection, Response & Recovery
Cyber Risk Management / Strategy | Governance | Business Context | Continuous Compliance

Native security controls are helpful but not sufficient, especially across multiple clouds or hybrid environments


DATA
SaaS / Data & App
PaaS / IAM & Cryptography
IaaS / Zero Trust Security for Infrastructure
Shared Responsibility / Threat Detection, Response & Recovery
Cyber Risk Management / Strategy | Governance | Business Context | Continuous Compliance

Cloud Native Capabilities

We’re hearing a lot of new cloud security concerns from customers. **Where do they start?**

How can I integrate my native security tools into my overall security operations?

What are my security responsibilities vs. my Cloud Service Provider’s?

How do I secure my critical data on cloud?

How can I get visibility into and manage Shadow IT usage?

How can I ensure my native security tools are properly configured?

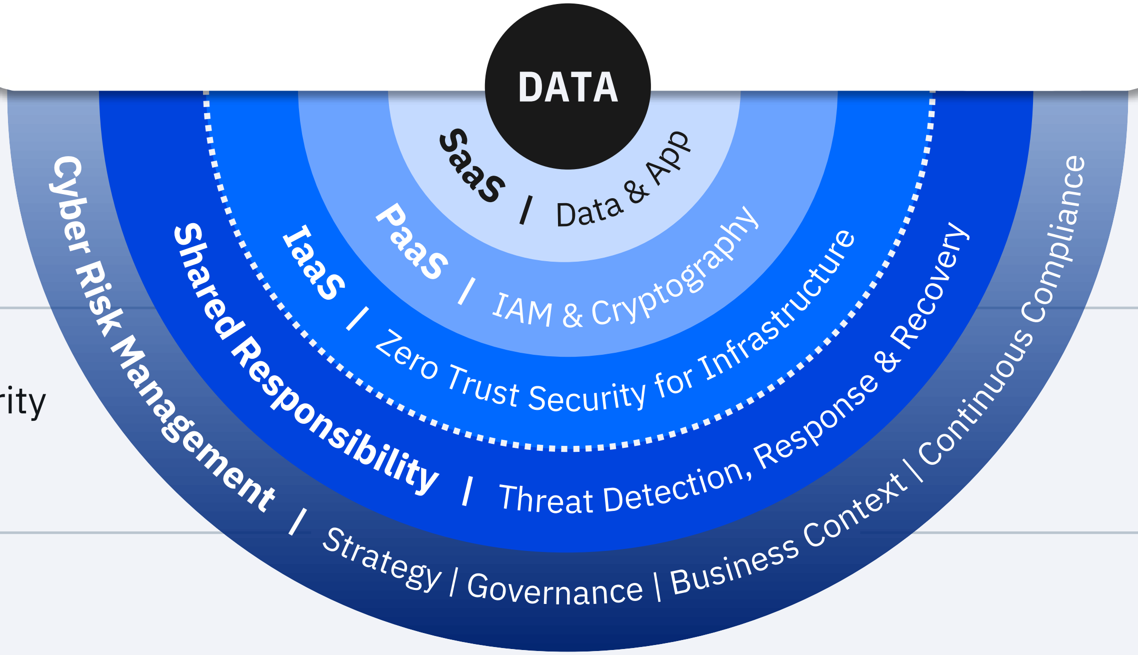
How do I centrally manage policy across my on-premise and cloud environments?

How do I develop cloud applications that are secure by design?

How do I secure access to my cloud workloads?

How do I keep up with changing compliance regulations?

How can I apply security without impacting the speed of business innovation?



DATA

SaaS / Data & App

PaaS / IAM & Cryptography

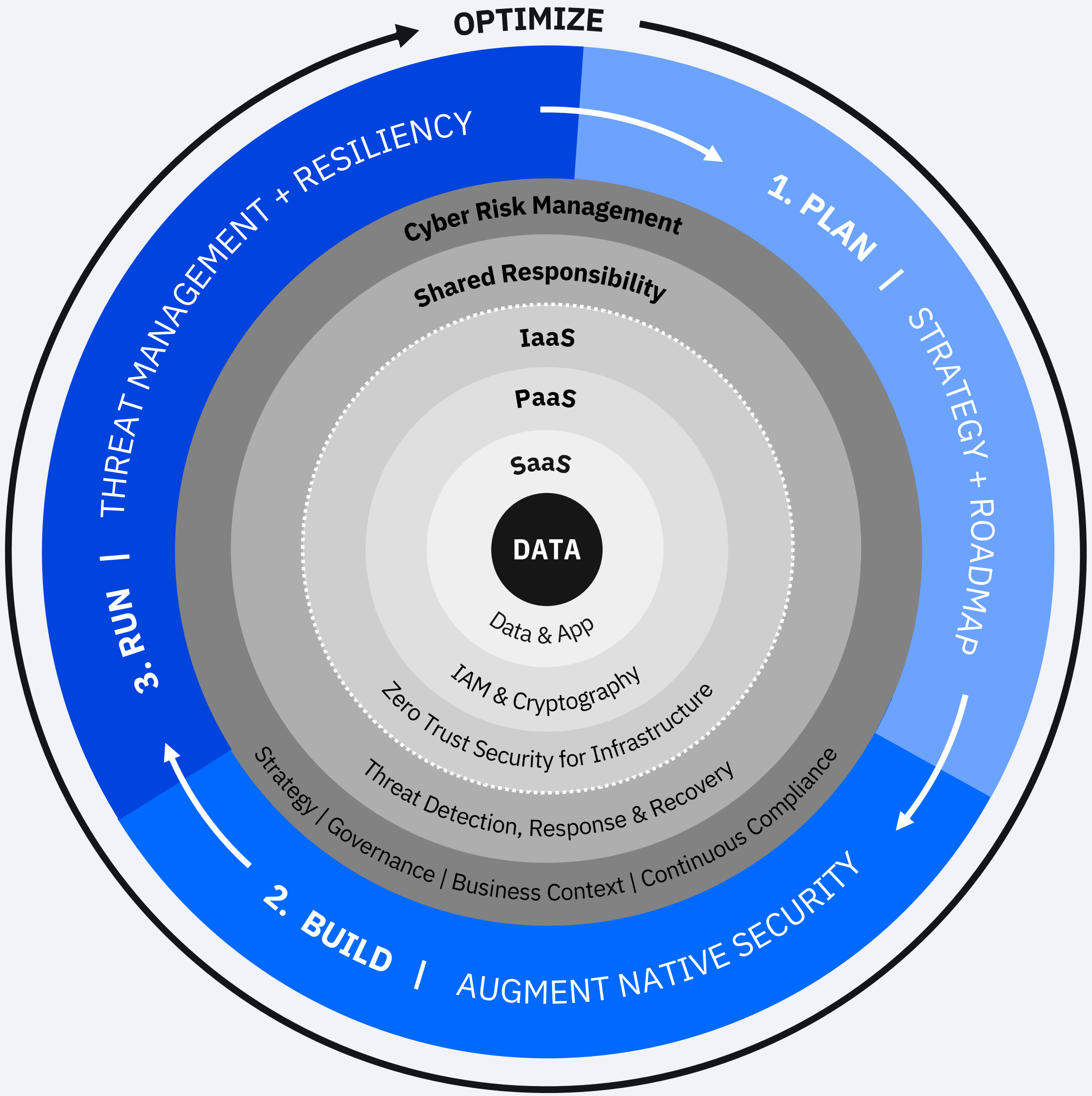
IaaS / Zero Trust Security for Infrastructure

Shared Responsibility / Threat Detection, Response & Recovery

Cyber Risk Management / Strategy | Governance | Business Context | Continuous Compliance

Introducing IBM X-Force Cloud Security Services

A programmatic approach to securing the hybrid enterprise


OPTIMIZE
1. PLAN / STRATEGY + ROADMAP
2. BUILD / AUGMENT NATIVE SECURITY
3. RUN / THREAT MANAGEMENT + RESILIENCY
Cyber Risk Management
Shared Responsibility
IaaS
PaaS
SaaS
DATA
Data & App
IAM & Cryptography
Zero Trust Security for Infrastructure
Threat Detection, Response & Recovery
Strategy / Governance | Business Context | Continuous Compliance

1. PLAN

Build a cloud security strategy and adoption roadmap

2. BUILD

Harden native cloud security + augment with additional security controls

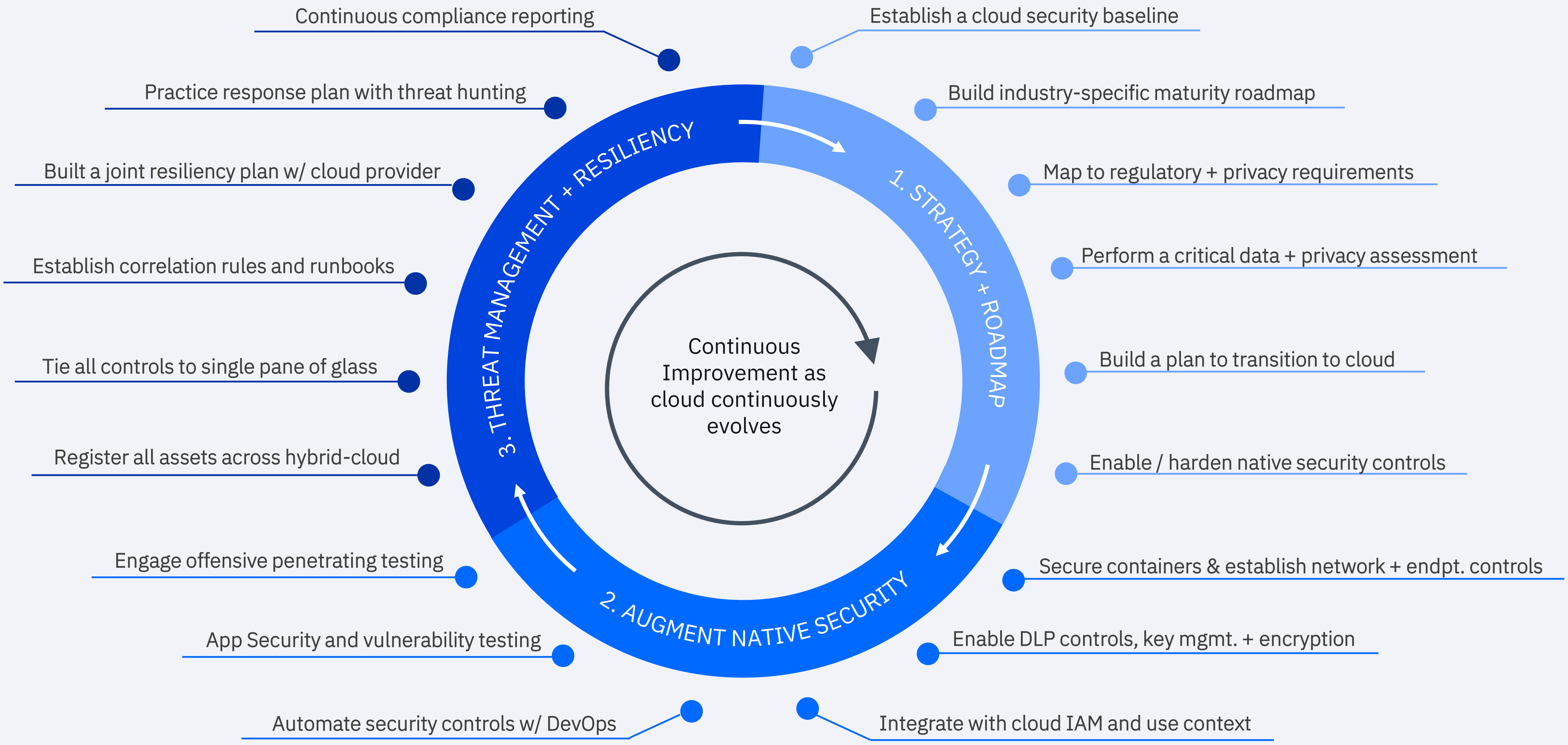
3. RUN

Provide threat management with an integrated resiliency plan

4. OPTIMIZE

Continuous improvement as cloud continuously evolves

A programmatic approach to securing the hybrid enterprise

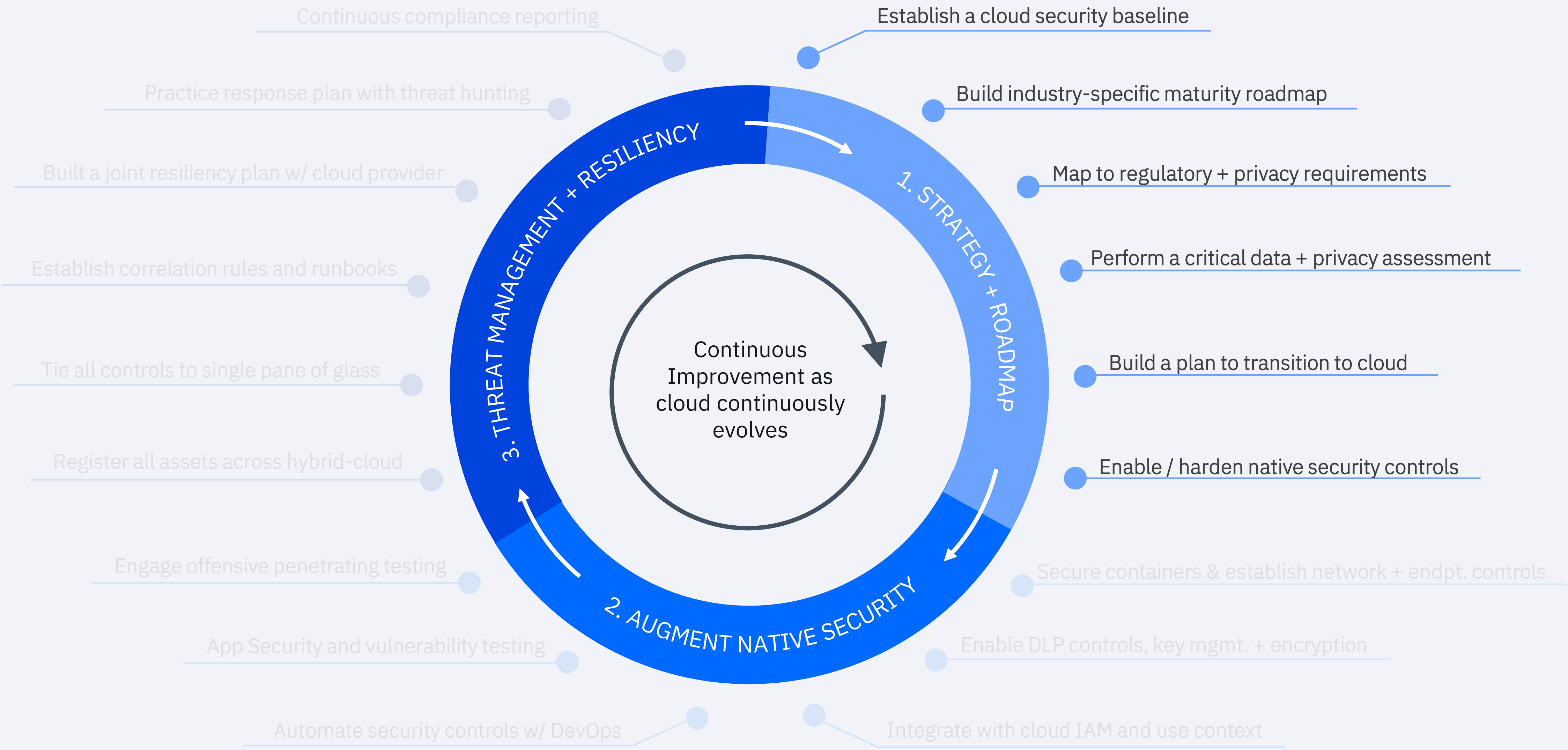

1. STRATEGY + ROADMAP
2. AUGMENT NATIVE SECURITY
3. THREAT MANAGEMENT + RESILIENCY
Continuous Improvement as cloud continuously evolves

1. Strategy + Roadmap
- Establish a cloud security baseline
- Build industry-specific maturity roadmap
- Map to regulatory + privacy requirements
- Perform a critical data + privacy assessment
- Build a plan to transition to cloud
- Enable / harden native security controls

2. Augment Native Security
- Secure containers & establish network + endpt. controls
- Enable DLP controls, key mgmt. + encryption
- Integrate with cloud IAM and use context
- Automate security controls w/ DevOps
- App Security and vulnerability testing
- Engage offensive penetrating testing

3. Threat Management + Resiliency
- Register all assets across hybrid-cloud
- Tie all controls to single pane of glass
- Establish correlation rules and runbooks
- Built a joint resiliency plan w/ cloud provider
- Practice response plan with threat hunting
- Continuous compliance reporting

A programmatic approach to securing the hybrid enterprise



1. STRATEGY + ROADMAP

2. AUGMENT NATIVE SECURITY

3. THREAT MANAGEMENT + RESILIENCY

Continuous Improvement as cloud continuously evolves

Establish a cloud security baseline

Build industry-specific maturity roadmap

Map to regulatory + privacy requirements

Perform a critical data + privacy assessment

Build a plan to transition to cloud

Enable / harden native security controls

Secure containers & establish network + endpt. controls

Enable DLP controls, key mgmt. + encryption

Integrate with cloud IAM and use context

Automate security controls w/ DevOps

App Security and vulnerability testing

Engage offensive penetrating testing

Register all assets across hybrid-cloud

Tie all controls to single pane of glass

Establish correlation rules and runbooks

Built a joint resiliency plan w/ cloud provider

Practice response plan with threat hunting

Continuous compliance reporting

Strategy + Roadmap

BASELINE
Establish a cloud security baseline

ROADMAP
Build industry-specific maturity roadmap

REGULATORY
Map to regulatory + privacy requirements

CRITICAL DATA
Perform a critical data assessment

TRANSITION PLAN
Build a plan to transition to cloud

NATIVE SECURITY
Enable / harden native security controls

It is critical to establish a Cloud Security Strategy, Governance + Readiness Plan

Our Cloud Security Strategy + Assessment can help you:

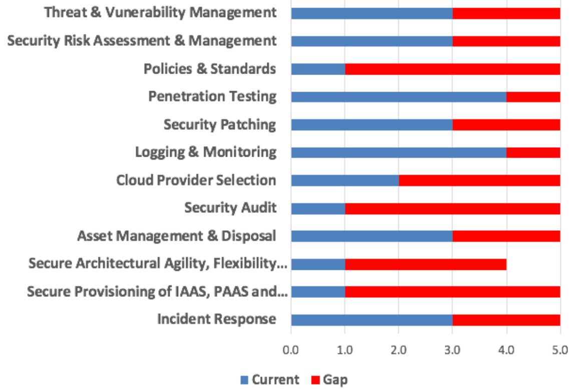
Assess your current state cloud security maturity

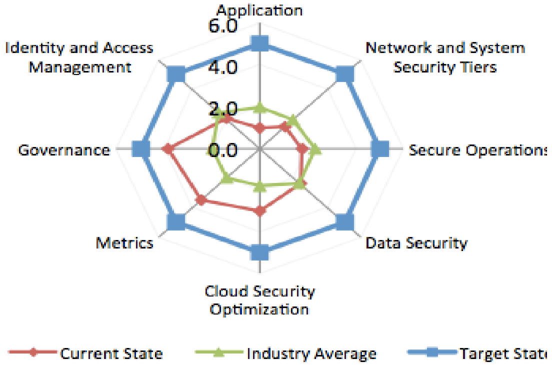
Define your future state that secures workloads across your hybrid environment

Build a strategy + roadmap for cloud migration that addresses pertinent security + regulatory concerns

A holistic assessment of current state security maturity:

- ✓ Governance
- ✓ Metrics
- ✓ Cloud Security Optimization
- ✓ Data Security
- ✓ Application Security
- ✓ Network and System Security
- ✓ Security Operations
- ✓ Identity + Access Management





Strategy + Roadmap

BASELINE
Establish a cloud security baseline

ROADMAP
Build industry-specific maturity roadmap

REGULATORY
Map to regulatory + privacy requirements

CRITICAL DATA
Perform a critical data assessment

TRANSITION PLAN
Build a plan to transition to cloud

NATIVE SECURITY
Enable / harden native security controls

If you don’t know what or where your critical data is, you can’t protect it.

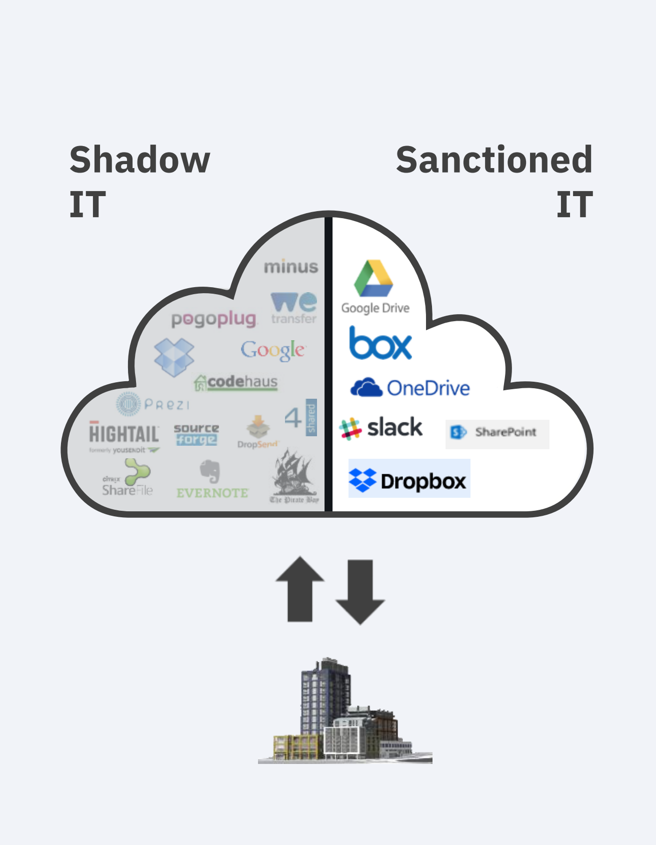
Organizations moving to cloud are now challenged with a fluid data perimeter.

Conduct a critical data assessment to understand:

✓ **WHAT:**
What is your most critical data
What regulated data exists

✓ **WHERE:**
Where these critical assets reside and if they are properly classified + protected

✓ **WHO:**
Who has access to your critical assets



Shadow IT Discovery

Gain a holistic understanding of what SaaS applications are used in your organization (sanction + Shadow IT)

Use policy based scanning to find instances of sensitive data including Personal Data, PHI, credit cards etc.

Misconfigured cloud services is one of the top reasons for data breaches.

It’s imperative to lock down your cloud environments and harden your native controls.

Our low-commitment, quick-start consulting engagements can help:

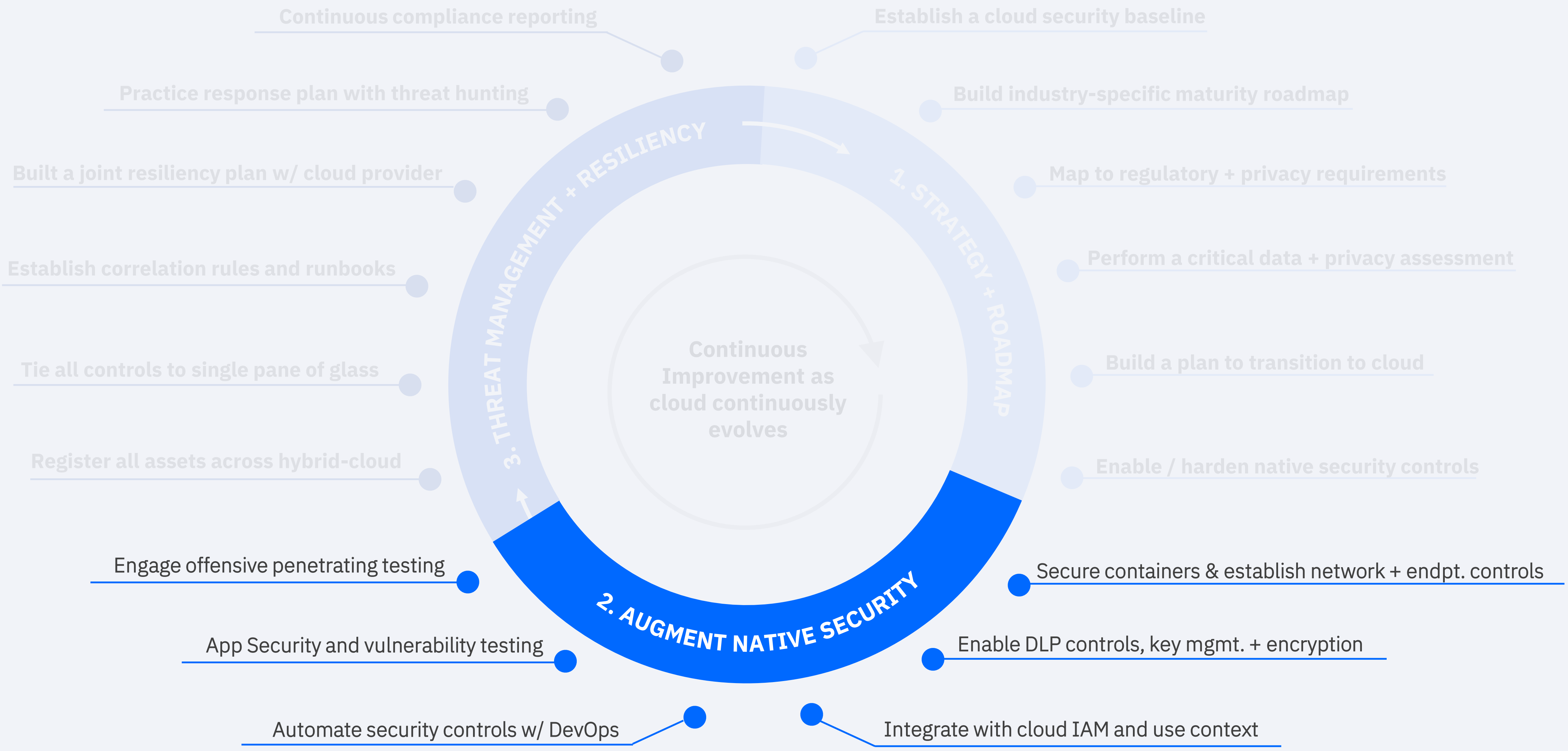
- Harden security posture of native cloud capabilities
- Align native security with threat management processes
- Streamline enterprise visibility for native security activity
- Enhance an organization’s readiness for cloud innovation
- Enable knowledge transfer for effective native security ops

Utilizing AWS native tools?

We offer the following quick-start engagements to help better secure your AWS cloud environment

1. AWS GuardDuty & Security Ops
2. AWS GuardDuty & Lambda
3. AWS Cloud Governance / Policy
4. Secure AWS Configurations
5. AWS Cloud Security Architecture

A programmatic approach to securing the hybrid enterprise



1. STRATEGY + ROADMAP

Establish a cloud security baseline

Build industry-specific maturity roadmap

Map to regulatory + privacy requirements

Perform a critical data + privacy assessment

Build a plan to transition to cloud

Enable / harden native security controls

2. AUGMENT NATIVE SECURITY

Secure containers & establish network + endpt. controls

Enable DLP controls, key mgmt. + encryption

Integrate with cloud IAM and use context

Automate security controls w/ DevOps

App Security and vulnerability testing

Engage offensive penetrating testing

3. THREAT MANAGEMENT + RESILIENCY

Register all assets across hybrid-cloud

Tie all controls to single pane of glass

Establish correlation rules and runbooks

Built a joint resiliency plan w/ cloud provider

Practice response plan with threat hunting

Continuous compliance reporting

Continuous Improvement as cloud continuously evolves

Augment Native Controls

ZERO TRUST
Establish zero-trust network + endpoint controls

DATA PROTECTION
Enable DLP controls, key management, & encryption

IDENTITY
Integrate with cloud IAM and user context

DEVSECOPS
Automate security controls w/ DevOps

SECURE BY DESIGN
Application Security + Vulnerability Testing

APP TESTING
Engage offensive testing

Extend beyond traditional network + endpoint security controls for more comprehensive coverage.

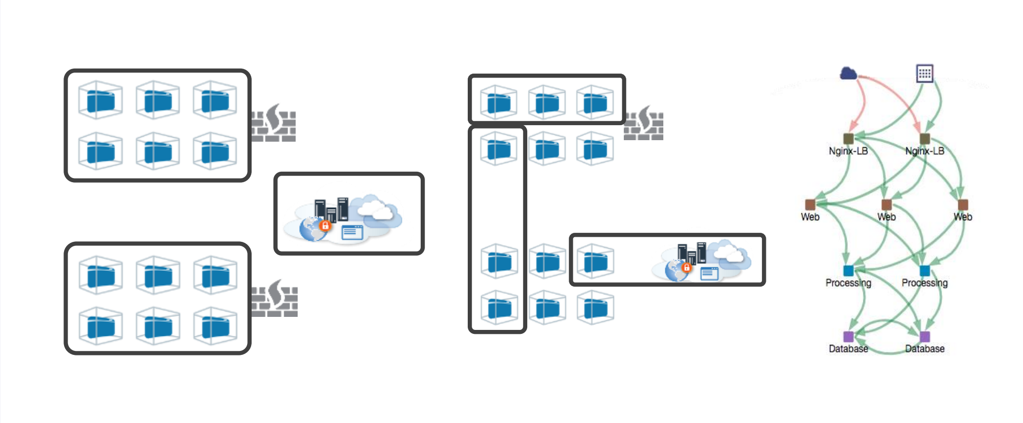
Micro-segmentation

Traditional networks:

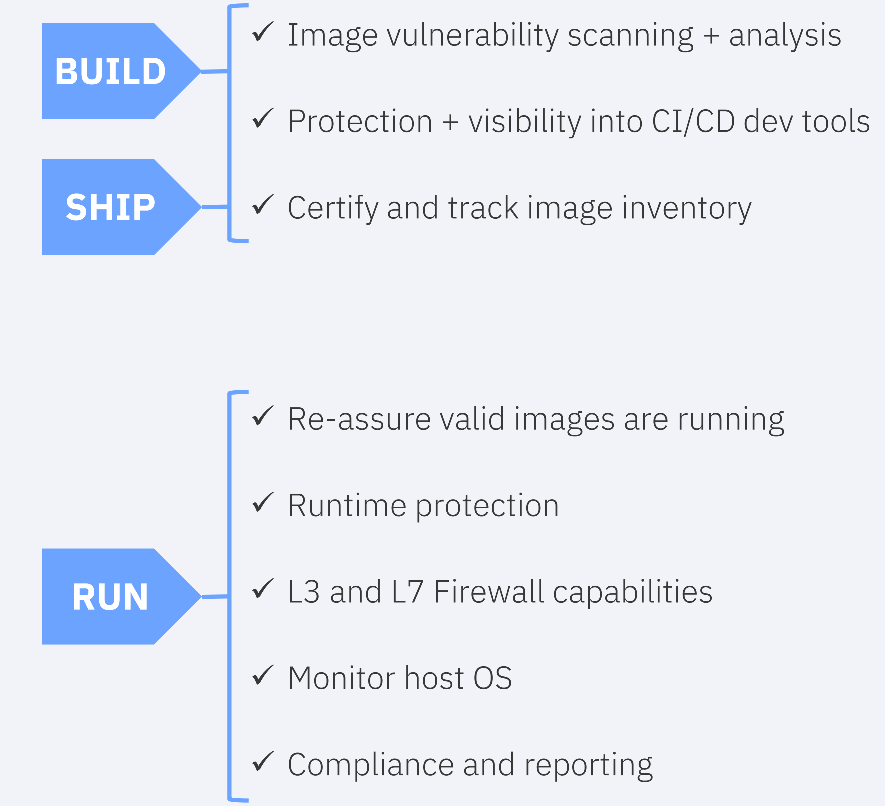
- **Little visibility** into application level traffic flows
- **Static policies** - harder to upkeep and can lead to application outages due to misconfiguration

Micro-segmentation:

- **Application-centric visibility** with more granular control
- **Adaptive** and can support hybrid environments



Container Security Services



BUILD

SHIP

- ✓ Image vulnerability scanning + analysis
- ✓ Protection + visibility into CI/CD dev tools
- ✓ Certify and track image inventory

RUN

- ✓ Re-assure valid images are running
- ✓ Runtime protection
- ✓ L3 and L7 Firewall capabilities
- ✓ Monitor host OS
- ✓ Compliance and reporting

Augment Native Controls

ZERO TRUST
Establish zero-trust network + endpoint controls

DATA PROTECTION
Enable DLP controls, key management, & encryption

IDENTITY
Integrate with cloud IAM and user context

DEVSECOPS
Automate security controls w/ DevOps

SECURE BY DESIGN
Application Security + Vulnerability Testing

APP TESTING
Engage offensive testing

Secure your critical data across your hybrid environment.

Now that you've identified your critical data, you must implement controls to protect it.

DLP in the Cloud

Sanctioned IT / SaaS:

- Use **policy based DLP** to protect sensitive assets from being copied to the cloud
- Sensitive data can be **blocked** from exfiltration, **quarantined**, or **deleted**.

Public Cloud:

- Scheduled processes to check for sensitive assets in public cloud

Cloud Data Encryption + Key Lifecycle Management

Driven by the need to support regulatory compliance

Can use either IBM or cloud native controls (AWS + Azure)

Key life-cycle management - BYoK or cloud-native

Augment Native Controls

ZERO TRUST
Establish zero-trust network + endpoint controls

DATA PROTECTION
Enable DLP controls, key management, & encryption

IDENTITY
Integrate with cloud IAM and user context

DEVSECOPS
Automate security controls w/ DevOps

SECURE BY DESIGN
Application Security + Vulnerability Testing

APP TESTING
Engage offensive testing

Assess your cloud IAM strategy + explore IDaaS solutions to optimize your technology investments

Moving workloads to cloud doesn’t necessarily mean changes to your IAM toolset

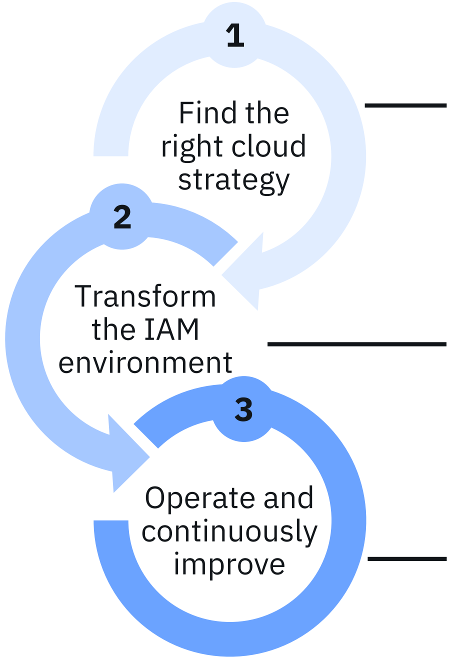
Can you extend your existing policies and controls to the new cloud workloads?

Use Case:
Can access to your cloud accounts be integrated as part of your privileged access management program?

Use Case:
Can your MFA be extended to internet-facing / accessible applications?

But many clients do want to move their IAM workloads to the cloud as well

Our **Journey to Cloud-Based IAM** solution approaches your IAM transformation in three stages:


1
Find the right cloud strategy
2
Transform the IAM environment
3
Operate and continuously improve

Design a solution focused on user outcomes using IBM Design Thinking

Optimize your technology investments by complementing existing IAM program with the cloud-based solution that fits your needs

Enhance your operational efficiency with improved business processes and Robotic Programming Automation (RPA)

Augment Native Controls

ZERO TRUST
Establish zero-trust network + endpoint controls

DATA PROTECTION
Enable DLP controls, key management, & encryption

IDENTITY
Integrate with cloud IAM and user context

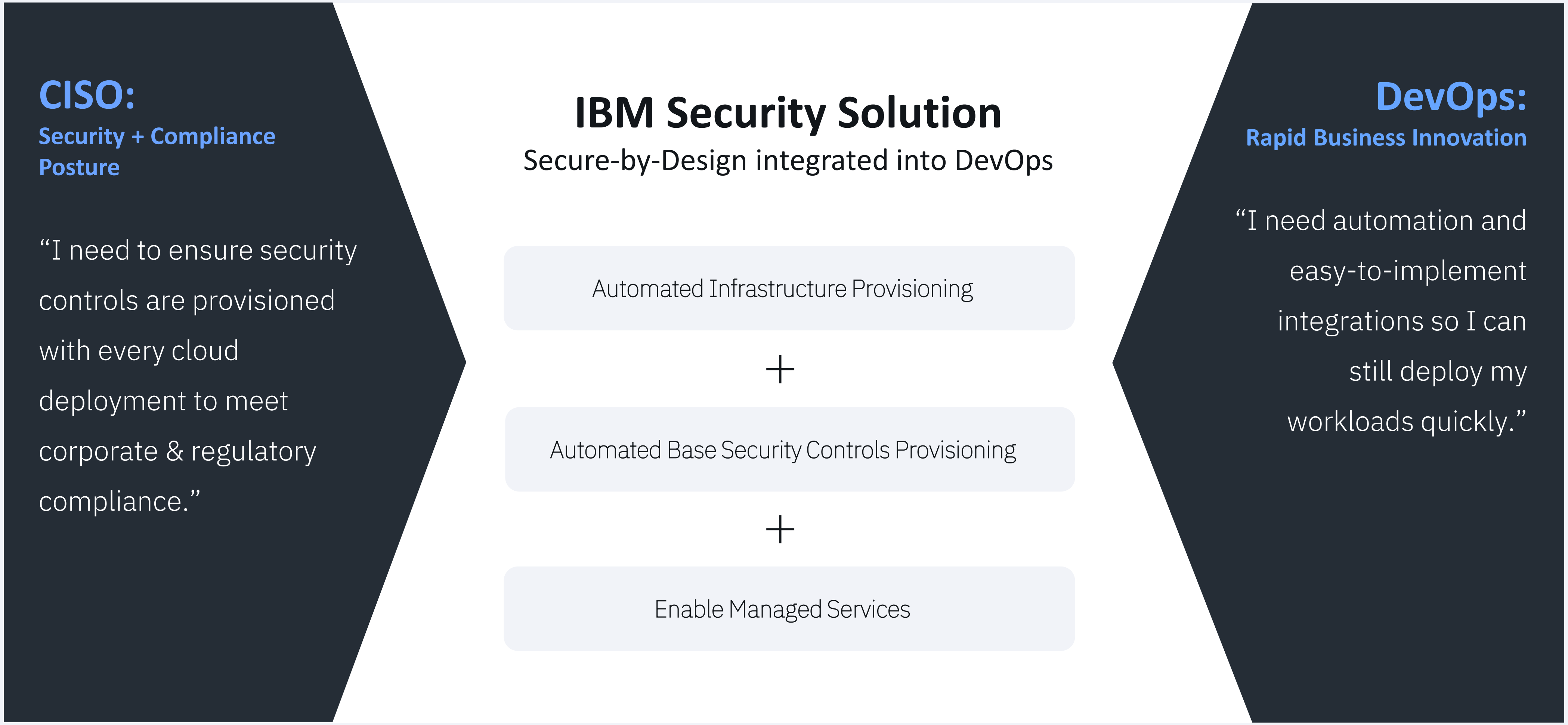
DEVSECOPS
Automate security controls w/ DevOps

SECURE BY DESIGN
Application Security + Vulnerability Testing

APP TESTING
Engage offensive testing

Emerging DevOps teams lead to conflicting objectives

You need a solution that can satisfy both sets of objectives



CISO:

Security + Compliance Posture

"I need to ensure security controls are provisioned with every cloud deployment to meet corporate & regulatory compliance."

IBM Security Solution

Secure-by-Design integrated into DevOps

Automated Infrastructure Provisioning

+

Automated Base Security Controls Provisioning

+

Enable Managed Services

DevOps:

Rapid Business Innovation

"I need automation and easy-to-implement integrations so I can still deploy my workloads quickly."

Augment Native Controls

ZERO TRUST
Establish zero-trust network + endpoint controls

DATA PROTECTION
Enable DLP controls, key management, & encryption

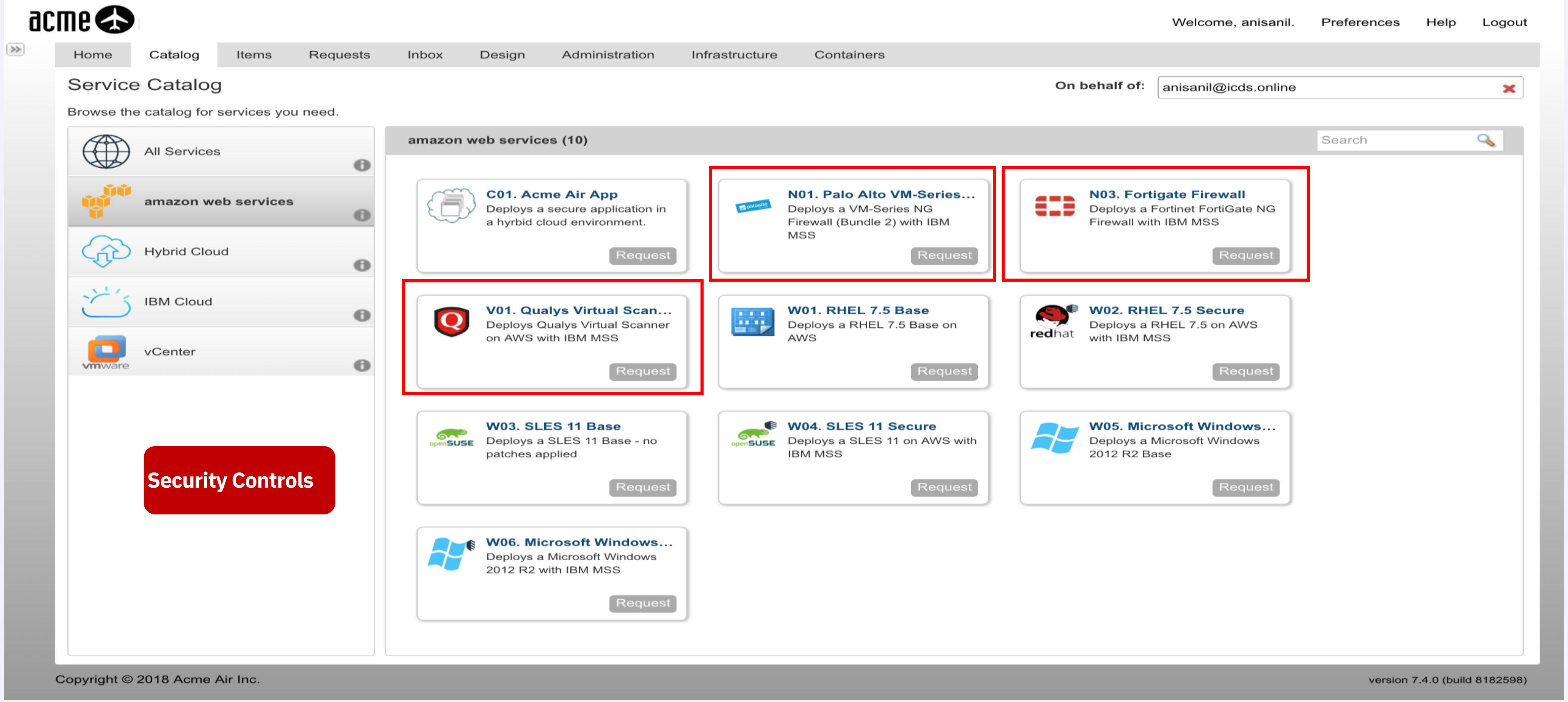
IDENTITY
Integrate with cloud IAM and user context

DEVSECOPS
Automate security controls w/ DevOps

SECURE BY DESIGN
Application Security + Vulnerability Testing

APP TESTING
Engage offensive testing

Keeping pace with DevOps: Deploying base security controls at cloud speed



acme

Welcome, anisanil. Preferences Help Logout

Home | Catalog | Items | Requests | Inbox | Design | Administration | Infrastructure | Containers

Service Catalog

On behalf of: anisanil@icds.online

Browse the catalog for services you need.

- All Services
- amazon web services
- Hybrid Cloud
- IBM Cloud
- vCenter

amazon web services (10)

Search

C01. Acme Air App
Deploys a secure application in a hyrbid cloud environment.
Request

N01. Palo Alto VM-Series...
Deploys a VM-Series NG Firewall (Bundle 2) with IBM MSS
Request

N03. Fortigate Firewall
Deploys a Fortinet FortiGate NG Firewall with IBM MSS
Request

V01. Qualys Virtual Scan...
Deploys Qualys Virtual Scanner on AWS with IBM MSS
Request

W01. RHEL 7.5 Base
Deploys a RHEL 7.5 Base on AWS
Request

W02. RHEL 7.5 Secure
Deploys a RHEL 7.5 on AWS with IBM MSS
Request

W03. SLES 11 Base
Deploys a SLES 11 Base - no patches applied
Request

W04. SLES 11 Secure
Deploys a SLES 11 on AWS with IBM MSS
Request

W05. Microsoft Windows...
Deploys a Microsoft Windows 2012 R2 Base
Request

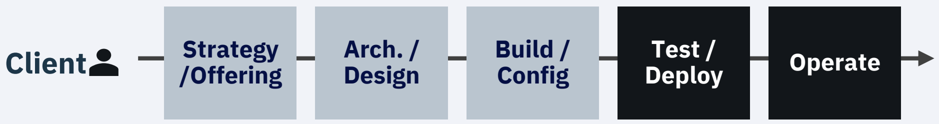
W06. Microsoft Windows...
Deploys a Microsoft Windows 2012 R2 with IBM MSS
Request

Security Controls

Copyright © 2018 Acme Air Inc.

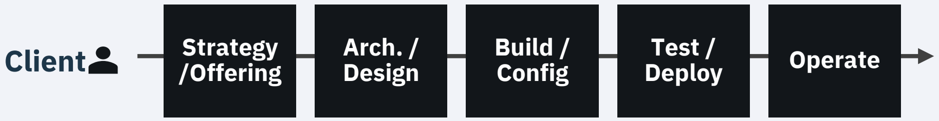
version 7.4.0 (build 8182598)

Current



Security brought in later

To be : Shift Left



Security embedded throughout the entire development lifecycle

Augment Native Controls

ZERO TRUST
Establish zero-trust network + endpoint controls

DATA PROTECTION
Enable DLP controls, key management, & encryption

IDENTITY
Integrate with cloud IAM and user context

DEVSECOPS
Automate security controls w/ DevOps

SECURE BY DESIGN
Application Security + Vulnerability Testing

APP TESTING
Engage offensive testing

Implement a secure-by-design application development methodology

Application Security Program Services

Secure-by-Design strategy + advisory services

Guidance with CI/CD implementation
Development standards, etc.

Secure Development Support Services

Providing support to the development organization across their various tasks + challenges

Non-functional security requirements gathering, remediation and implementation support, etc.

Secure Development Training Services

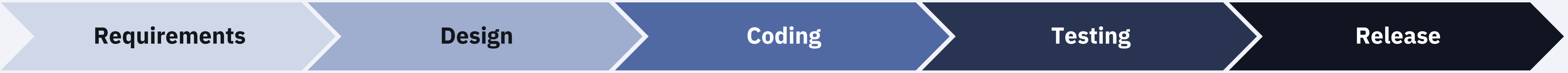
Secure development training & coding language best practices

Application Security Testing Services

Full suite of tools and processes around to help identify vulnerabilities early

Pre and post production penetration testing

Application Security solutions to support clients across their entire SDLC



Augment Native Controls

ZERO TRUST
Establish zero-trust network + endpoint controls

DATA PROTECTION
Enable DLP controls, key management, & encryption

IDENTITY
Integrate with cloud IAM and user context

DEVSECOPS
Automate security controls w/ DevOps

SECURE BY DESIGN
Application Security + Vulnerability Testing

APP TESTING
Engage offensive testing

X-Force Red Independent Application Security Testing

Test your applications to defend against attacks

Why Application Testing?

- ✓ Identify critical vulnerabilities that scanning tools cannot find
- ✓ Understand the behaviors of applications, how they communicate and how attackers could circumvent the logic
- ✓ Identify processes developers may have overlooked
- ✓ Make programmatic changes to strengthen security across the entire environment
- ✓ Understand where to invest security spend so that residual loss is minimized

Application Testing from X-Force Red

Application Vulnerability Assessment

- Scan + manual poke & prod to validate vulnerabilities, weed out false positives + identify add’l vulnerabilities
- Raw, automated, static scanning

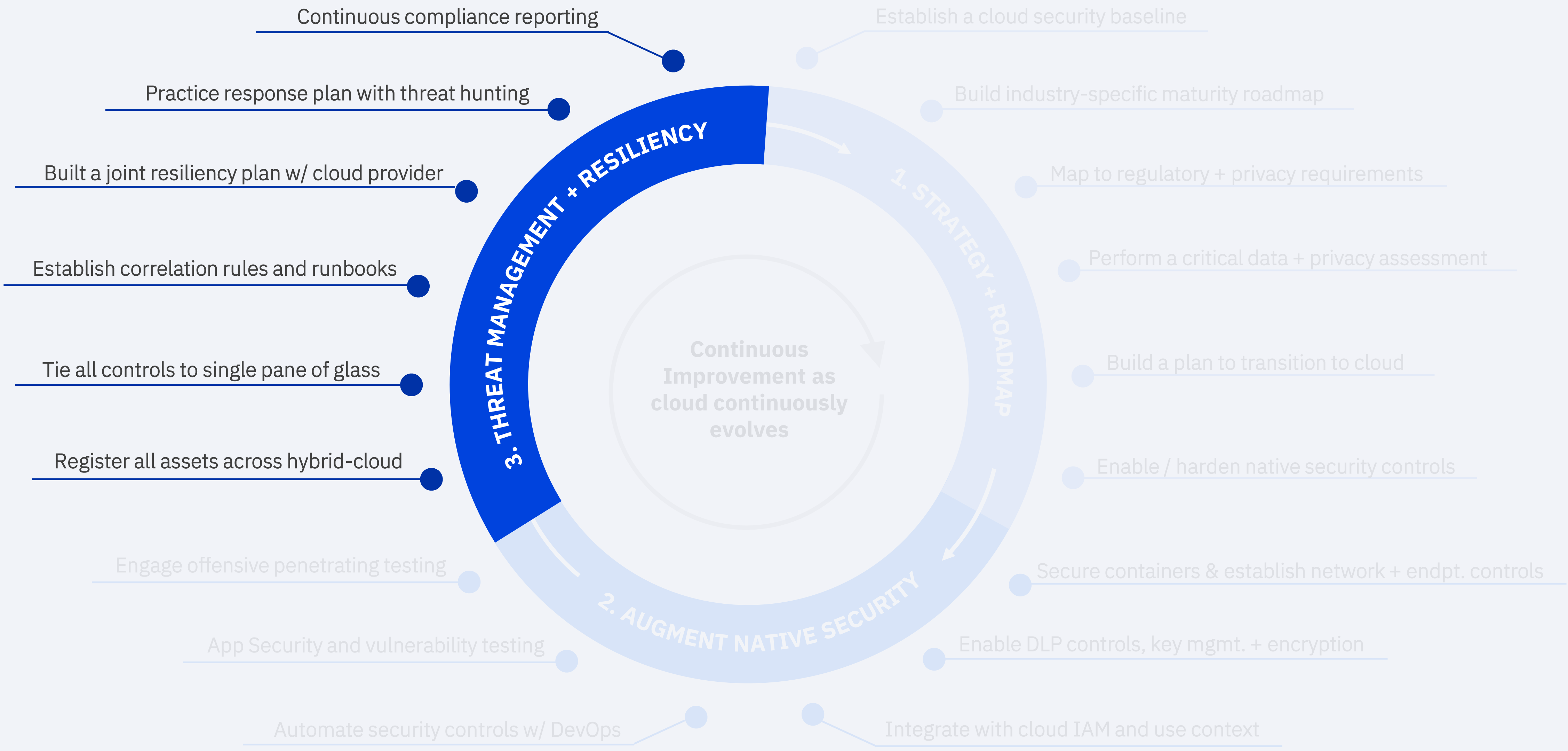
Application Penetration Testing

- Manual testing to find “as of yet unknown” vulnerabilities that only human testers can find

Application Source Code Review

- Manual analysis and static code review

A programmatic approach to securing the hybrid enterprise



Continuous compliance reporting

Practice response plan with threat hunting

Built a joint resiliency plan w/ cloud provider

Establish correlation rules and runbooks

Tie all controls to single pane of glass

Register all assets across hybrid-cloud

Engage offensive penetrating testing

App Security and vulnerability testing

Automate security controls w/ DevOps

Establish a cloud security baseline

Build industry-specific maturity roadmap

Map to regulatory + privacy requirements

Perform a critical data + privacy assessment

Build a plan to transition to cloud

Enable / harden native security controls

Secure containers & establish network + endpt. controls

Enable DLP controls, key mgmt. + encryption

Integrate with cloud IAM and use context

3. THREAT MANAGEMENT + RESILIENCY
1. STRATEGY + ROADMAP
2. AUGMENT NATIVE SECURITY
Continuous Improvement as cloud continuously evolves

Threat Management + Resiliency

ASSET INVENTORY
Register all assets across hybrid-cloud

VISIBILITY
Tie all controls to a single pane of glass

RUNBOOKS
Establish correlation rules and runbooks

RESILIENCY
Build a joint resiliency plan w/ cloud provider

THREAT HUNTING
Practice response plan with threat hunting

COMPLIANCE
Continuous compliance reporting

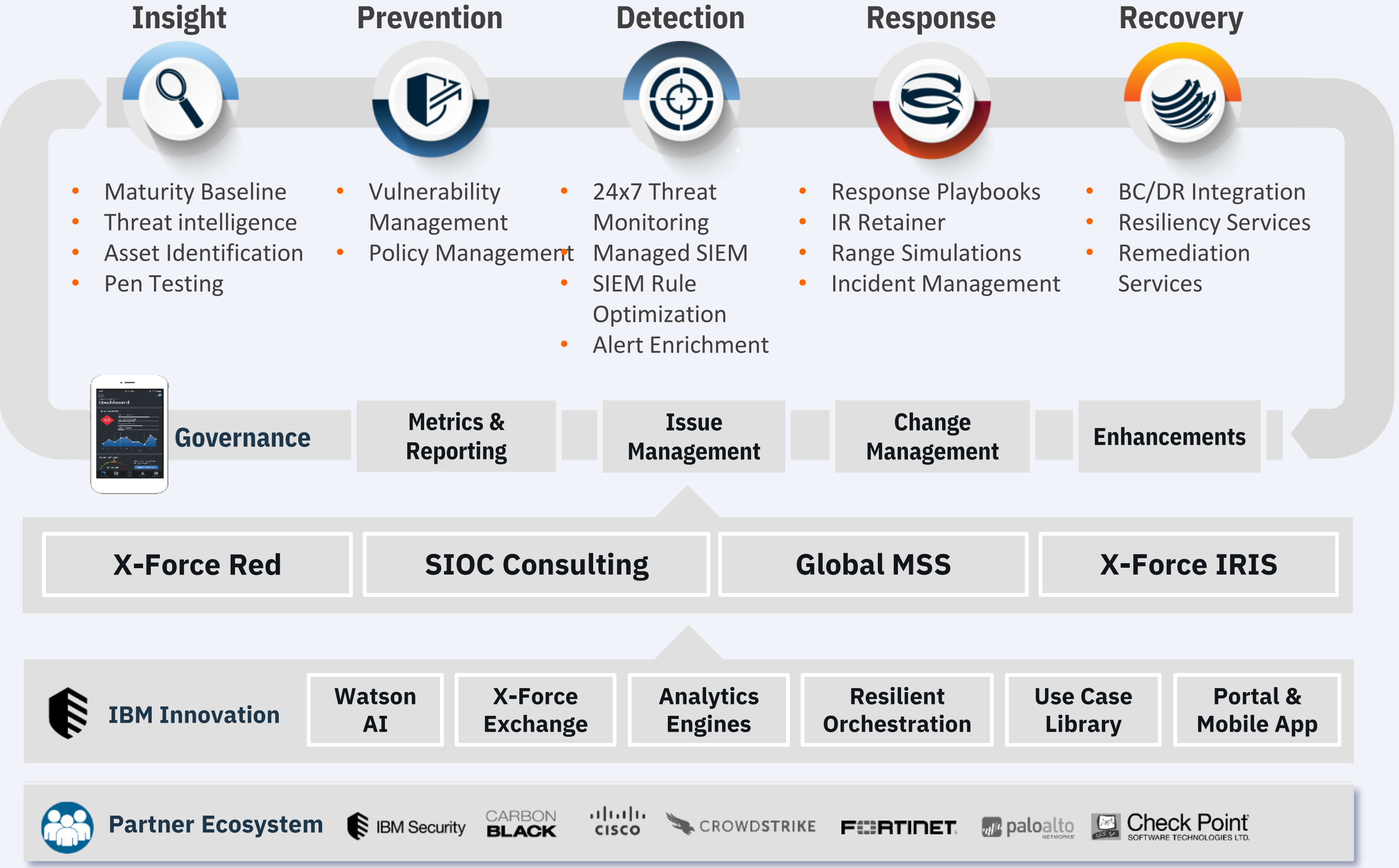
Introducing X-Force Threat Management

A smarter security solution to manage the 360 degree threat lifecycle

A programmatic framework leads to a prescriptive integrated approach that drives better results.

A trusted security partner with world class experts that can bring critical insight and scale.

A smarter platform that can accelerate investigation and response with analytics, AI and orchestration.



Insight
- Maturity Baseline
- Threat intelligence
- Asset Identification
- Pen Testing

Prevention
- Vulnerability Management
- Policy Management

Detection
- 24x7 Threat Monitoring
- Managed SIEM
- SIEM Rule Optimization
- Alert Enrichment

Response
- Response Playbooks
- IR Retainer
- Range Simulations
- Incident Management

Recovery
- BC/DR Integration
- Resiliency Services
- Remediation Services

Governance | Metrics & Reporting | Issue Management | Change Management | Enhancements

X-Force Red | SIOC Consulting | Global MSS | X-Force IRIS

IBM Innovation: Watson AI | X-Force Exchange | Analytics Engines | Resilient Orchestration | Use Case Library | Portal & Mobile App

Partner Ecosystem

Threat Management + Resiliency

ASSET INVENTORY
Register all assets across hybrid-cloud

VISIBILITY
Tie all controls to a single pane of glass

RUNBOOKS
Establish correlation rules and runbooks

RESILIENCY
Build a joint resiliency plan w/ cloud provider

THREAT HUNTING
Practice response plan with threat hunting

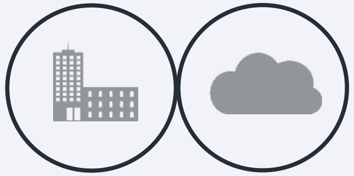
COMPLIANCE
Continuous compliance reporting

Operating in a hybrid environment often leads to disparate controls.

You need to centralize security visibility for policy management

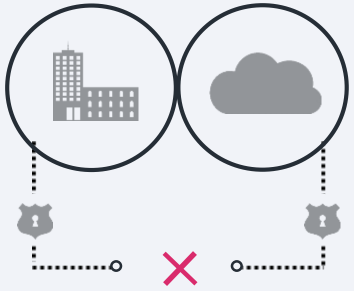
You have....

Workloads **on premise** + **on cloud(s)**



With....

Disparate security controls across both



We bring....

Logs & alerts into a **single pane of glass** via our VSOC portal

Providing....

Threat Management

Incident Management

Log Management & Alerting

Ticketing

Centrally through our MSS VSOC Portal

Cloud Agnostic

Supporting workloads across:

IBM aws Azure vmware **On Premise**

Vendor Agnostic

Supporting multiple best-of-breed technologies across multiple cloud environments & on-premise

Threat Management + Resiliency

ASSET INVENTORY
Register all assets across hybrid-cloud

VISIBILITY
Tie all controls to a single pane of glass

RUNBOOKS
Establish correlation rules and runbooks

RESILIENCY
Build a joint resiliency plan w/ cloud provider

THREAT HUNTING
Practice response plan with threat hunting

COMPLIANCE
Continuous compliance reporting

Compliance doesn’t stop at the cloud.

There are hundreds of mandatory laws and regulations, as well as voluntary standards, audit standards, codes of conduct and internal policies that companies have to comply with.

Strategy Development

Not sure where to start?
Let us help you assess your current state cloud controls maturity against relevant regulatory requirements, and define a strategy for improving and managing your compliance posture.

Tool-Based Solution

Not in a highly regulated industry?
Some use-cases can be solved with simple tooling. We can help design and implement a tool-based compliance approach with tools such as Dome9.

Fully Managed

Highly regulated or operating across multiple jurisdictions?
Our managed Technology Compliance Advisor service can help map your existing controls to relevant regulatory requirements, and then regularly assessing for updates & notify you of required actions.

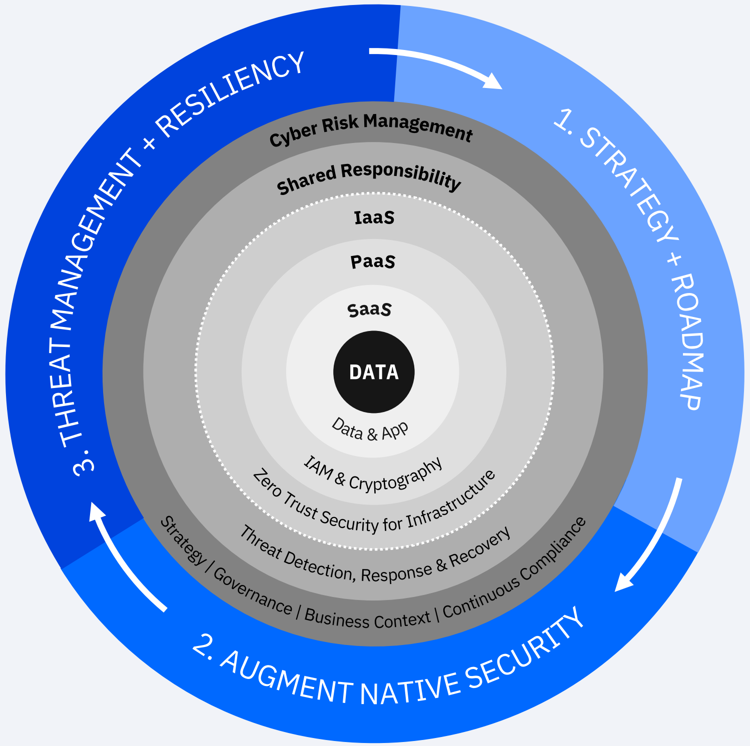
The legal and regulatory landscape is always changing.

How can you ensure rigorous compliance for cloud workloads?

$$

The financial impacts of non-compliance are large and rising.

Moving to cloud introduces a series of new challenges and IBM X-Force Cloud Security Services can help


1. STRATEGY + ROADMAP
2. AUGMENT NATIVE SECURITY
3. THREAT MANAGEMENT + RESILIENCY
Cyber Risk Management
Shared Responsibility
IaaS
PaaS
SaaS
DATA
Data & App
IAM & Cryptography
Zero Trust Security for Infrastructure
Threat Detection, Response & Recovery
Strategy | Governance | Business Context | Continuous Compliance

IBM Security brings a full package solution, with differentiated capabilities through our unique intellectual assets

- ✓ Assessment Framework
- ✓ Maturity Plan
- ✓ DevSecOps
- ✓ Regulatory Library
- ✓ Controls Hardening Library
- ✓ Use Case Library
- ✓ Offensive Testing
- ✓ Machine Learning
- ✓ Threat Intelligence
- ✓ Response Playbook

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM