Building a cloud security program that accelerates growth and business innovation

Amanda Sherman

Product Manager, IBM Security Services for Cloud

IBM Security

aweber@us.ibm.com

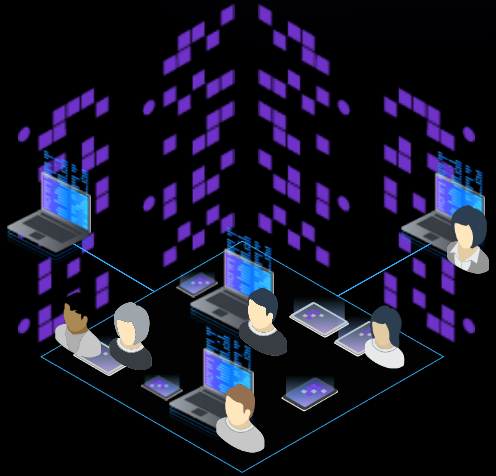
IBM **Security**

Digital transformation is accelerating

Businesses are embracing cloud to gain agility, competitive advantage & drive innovation

Applications & Data

Data is a shared resource for users and applications



Users & Endpoints

Accessing for anywhere using any device

Infrastructure

Servers and networks distributed across hybrid cloud environments

Yet often, the first **security** move to cloud is a lift-and-shift reaction which does not translate well

On Premise…

Complete control over privileged apps & access

Applications built within a defined perimeter

Trusted corporate network

Contained / limited data movement

In Cloud…

X Dynamic access from multiple access points and user groups

X Exposure of lax application security practices

X Internet-exposed management controls

X Static, incomplete data controls now paired up against dynamic workloads and data movement

This approach is creating many new security challenges.

Adapting Security Strategy for Multi-cloud

42%

believe they have effective multicloud security [1]

New Tools, Unfamiliar Technologies

85

security products across 40 different vendors [2]

Greater Risk for Misconfigurations

99%

Of cloud security failures will be the customer's fault [3]

Increasing Skills Shortage

1.8M

Unfilled cybersecurity jobs by 2022 [4]

Siloed Visibility To Threats

$3.86M

Global average cost of a data breach [5]

Securing Critical Data & Managing Access

~ ½

Of world's stored data expected to reside in public cloud by 2025 [6]

Expanding Threat Landscape

94%

Of organizations have multiple clouds [7]

Competitors Innovating Faster

63K+

Security incidents through exploitation of enterprise apps

[1] IBV Cloud Security Study 2021
[2] Thousands of IBM Security Services engagements
[3] Gartner, Innovation Insight for Cloud Security Posture Mgmt 2019
[4] Frost & Sullivan 2017 Study
[5] Ponemon Institute's 2020 Cost of a Data Breach Report
[6] IDC White Paper - #US44413318 Sponsored by Seagate
[7] Cloud Computing Trends: 2019 State of the Cloud Survey, Flexera

Security cannot be approached differently across your on premise and cloud environments. Instead, you need:

Consistent security controls and architecture

+

Centralized visibility to threats & compliance

1 Define a Cloud Strategy & Governance Program

Gap Analysis | Roadmap | Risk & Compliance | Cloud Native

2 Consistent Policy to Protect Workloads

Policy | Config | Compliance | Vulnerability | Threat

3 Detect & Respond to Cloud Misconfigurations

Policy | Compliance | Guardrails | Audit | Threat

4 Enable Dynamic Network & Access Controls

Network & ZTNA | Microsegmentation | MFA | PAM | Adaptive Access

5 Protect Data Wherever it Resides

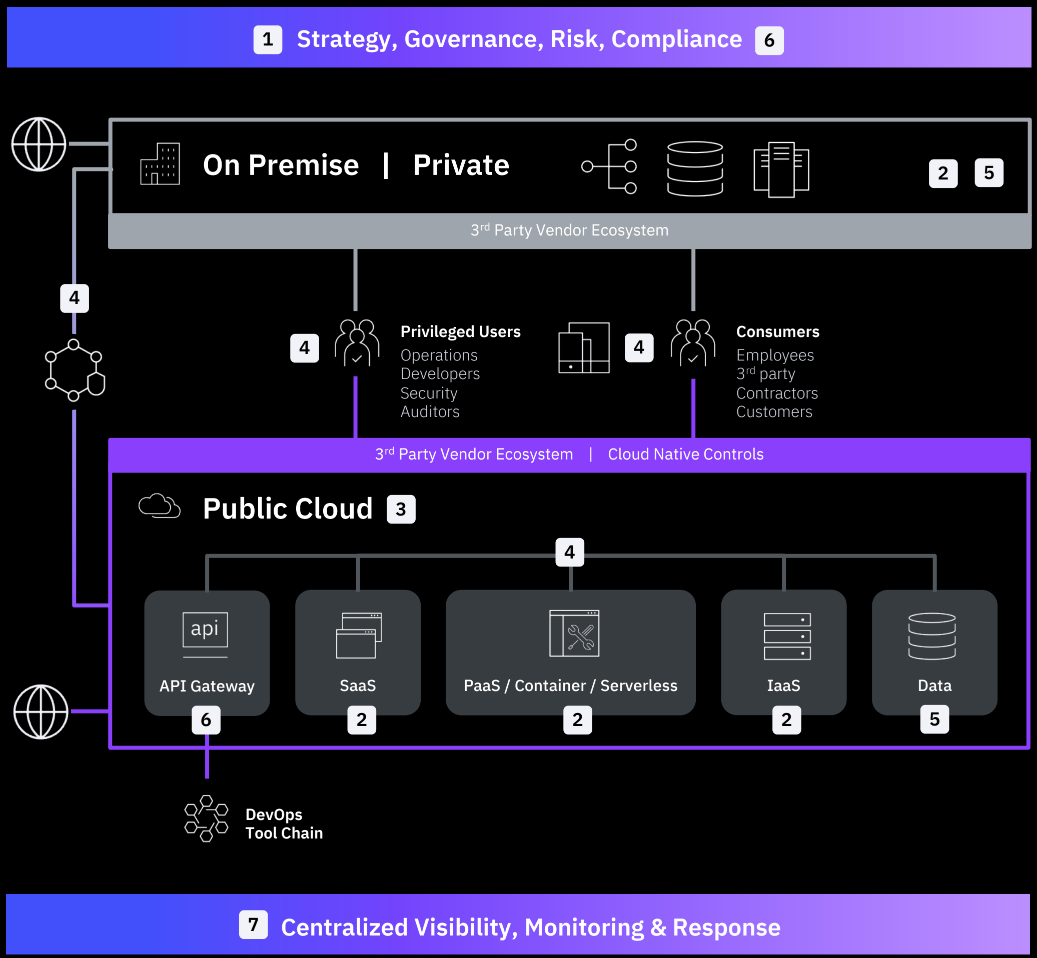
Discover & Classify | Key Mgmt. | Encryption | DLP | DAM

6 Modernize and Secure App Dev Processes

DevSecOps | SAST/DAST | API Security | Offensive Testing

7 Establish Centralized Threat Mgmt. Program

Vulnerability | Protection, Detection & Response | Use-Case Mgmt.



1 Strategy, Governance, Risk, Compliance 6

On Premise | Private 2 5

3rd Party Vendor Ecosystem

4

4 Privileged Users
Operations
Developers
Security
Auditors

4 Consumers
Employees
3rd party
Contractors
Customers

3rd Party Vendor Ecosystem | Cloud Native Controls

Public Cloud 3

4

API Gateway 6

SaaS 2

PaaS / Container / Serverless 2

IaaS 2

Data 5

DevOps
Tool Chain

7 Centralized Visibility, Monitoring & Response

Securing the hybrid multi-cloud enterprise requires an approach that is:

- ✓ Adaptive
- ✓ Programmatic
- ✓ Zero-Trust centric

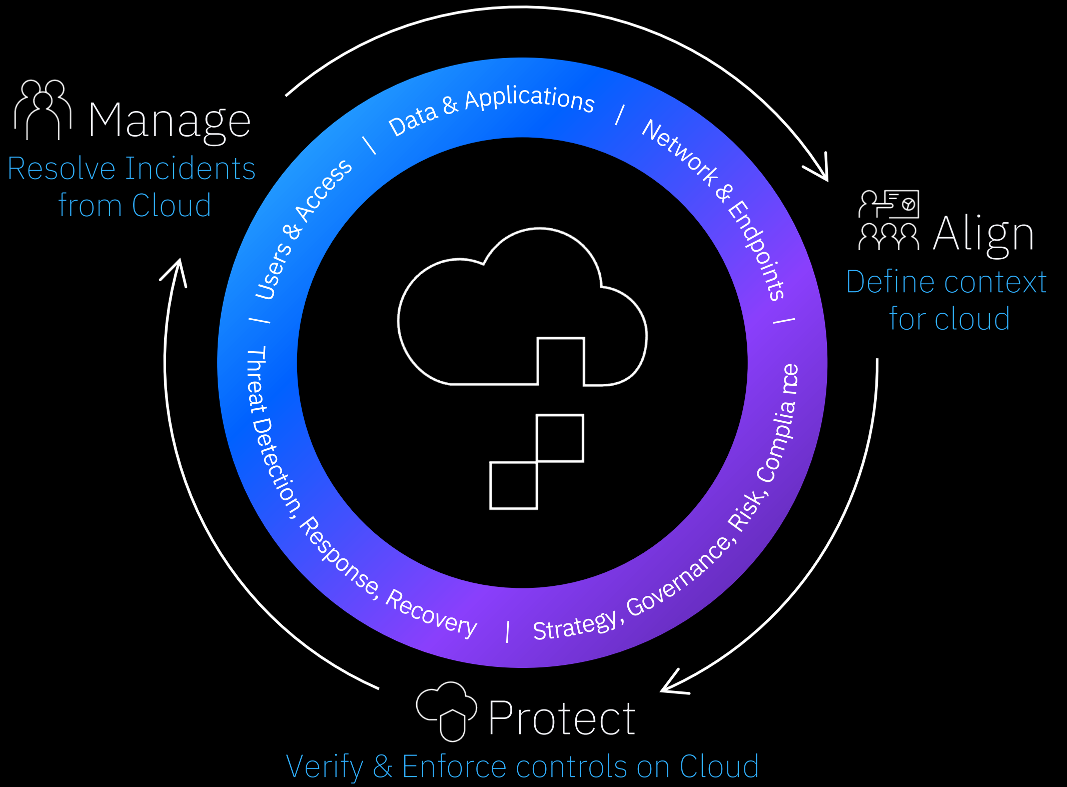
And that can:

Align security & cloud business strategies & goals

Protect digital users, assets, & data as you move and build on cloud

Manage defenses against growing hybrid cloud cyberthreats

Modernize security approach through automation, orchestration, and use of an open platform to better support the needs of the business



Manage
Resolve Incidents from Cloud

Align
Define context for cloud

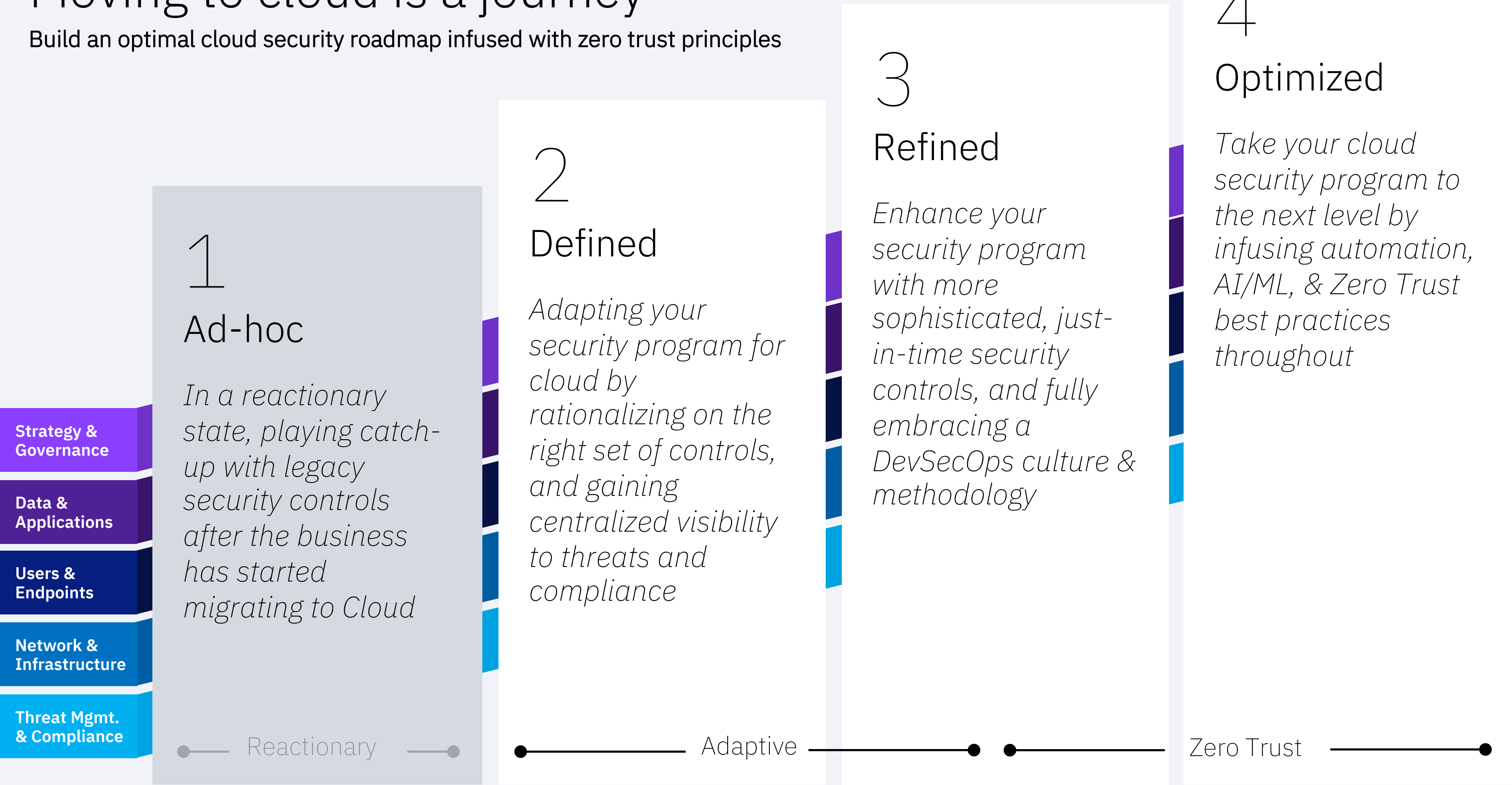
Protect
Verify & Enforce controls on Cloud

Users & Access / Data & Applications / Network & Endpoints / Strategy, Governance, Risk, Compliance / Threat Detection, Response, Recovery /

Modernize
Analyze & improve security & compliance posture

Moving to cloud is a journey

Build an optimal cloud security roadmap infused with zero trust principles



Strategy & Governance

Data & Applications

Users & Endpoints

Network & Infrastructure

Threat Mgmt. & Compliance

1 Ad-hoc

In a reactionary state, playing catch-up with legacy security controls after the business has started migrating to Cloud

2 Defined

Adapting your security program for cloud by rationalizing on the right set of controls, and gaining centralized visibility to threats and compliance

3 Refined

Enhance your security program with more sophisticated, just-in-time security controls, and fully embracing a DevSecOps culture & methodology

4 Optimized

Take your cloud security program to the next level by infusing automation, AI/ML, & Zero Trust best practices throughout

Reactionary

Adaptive

Zero Trust

ALIGN your cloud security program

DEFINE

Must-Have Top 3

1. **A defined *cloud* security strategy**
   Security baseline | Roadmap aligned to business & regulatory reqt's | Native vs. 3rd Party rationalization

2. **Discovery and classification of critical data & who has access to it**
   Crown jewels identified | Shadow IT Discovery | Data classified based on risk

3. **Centralized Threat Management & Compliance strategy**
   Configuration Drift Monitoring | All cloud & non-cloud workloads centrally managed

REFINE & OPTIMIZE

Should-Have

- Macro-level architectures across security domains
- Secure development practices implemented
- Optimal offensive testing strategy defined
- Deep resiliency plans in place with cloud vendors & 3rd party risk management strategy established

PROTECT digital users, data, & assets

DEFINE

Must-Have Top 3

1. **Implement granular, just-in-time controls**
   Across Data, IAM, Network segmentation, Endpoint & SOC controls & processes

2. **Fully embed security into application development**
   DevSecOps culture transformation | Secure-by-Design application development | API Security

3. **Centralized Cloud-Native Compliance Monitoring**
   Configuration Drift Monitoring (CSPM) | Secure cloud-native workloads

REFINE & OPTIMIZE

Should-Have

- Centralized policy engine allows for integrated decisions across planes and security domains to grant or deny access
- Automated security provisioning with DevOps
- Full risk quantification & context defined across all users, data, network & workloads
- Systems communicate & share info to make trusted decisions. Trust level defines required authentication method.

MANAGE & monitor hybrid cloud threats

DEFINE

Must-Have Top 3

1. **Centralized Threat Management visibility**
   All cloud & non-cloud workloads centrally managed across vulnerability mgmt., correlation & events, & response

2. **Centralized incident response capability**
   Clear integration & playbooks aligned with cloud security vendors

3. **Automated runbooks via Orchestration tools**
   Fully automated run-books and reconciliation via orchestration tools

REFINE & OPTIMIZE

Should-Have

- Continuous compliance monitoring & reporting
- Build a joint resiliency plan with cloud vendor(s)
- Practice threat hunting and incident response plan
- Fully automated and regulated cloud security provisioning
- Automation & AI being used for integrated context-driven correlation, insights & actions

Take our free, online Cloud Security Self-Assessment

https://ibm.biz/cloud-sec-maturity

Learn more about our Security Services and Solutions for Cloud

https://ibm.com/security/services/cloud-security-services

With much to consider, be sure to cover the basics

01

Assess your current environment & strategy

02

Understand what and where your critical data is

03

Review your current cloud compliance posture

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

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 **Security**

When you interact with IBM, this serves as your authorization to MESA - HITS Summit or its vendor to provide your contact information to IBM in order for IBM to follow up on your interaction. IBM's use of your contact information is governed by the IBM privacy Policy.

IBM

IBM