

IBM Security Services for Cloud

Protecting the hybrid multi-cloud

Presenter's name

Title

Cloud has
turned traditional
cybersecurity on its
head



of cloud security
failures will be the
organization's fault

\$474
Billion

Global Cloud
Revenue to Total
\$474 Billion in
2022*



\$3.8M

Global average
cost of a data
breach



of world's stored
data expected to
reside in public
cloud by 2025



Unanticipated Acceleration to Cloud

Pandemic accelerated change
and demand to allow users to
access the enterprise from
anywhere using any device



Regulatory Compliance Churn & Governance

With the migration of workloads to
the Cloud, Security, and
compliance are top-of-mind
across hybrid multi-cloud
environments



Disparate Controls & Decentralized Management

New computing approaches, including
Edge & multi-cloud, require robust
security platforms that can deploy
controls consistently & seamlessly



Growing Attack Surface & Threat Landscape

Growing threats, tools and data
inhibit security operations across
hybrid environments

Securing the hybrid enterprise requires a comprehensive cloud security program



- 01** Defining and implementing a Cloud Security Strategy
Comprehensive, Consistent & Zero Trust Centric



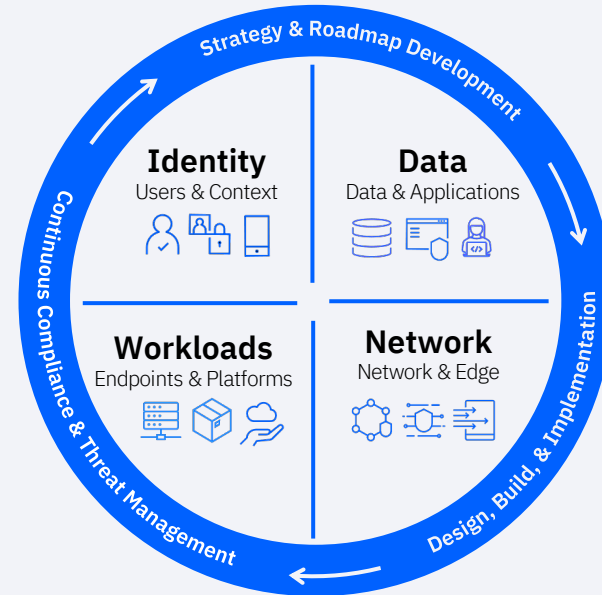
- 02** Enforcing policies to protect cloud resources



- 03** Ensuring security posture & compliance needs are continually met



- 04** Centralizing detection & response to threats 24x7



IBM Security Services for Cloud Services Framework

Services & Delivery Models

Advisory

- Cloud Security Assessment
- Cloud Security Strategy

Integration

- Secure Architecture Foundations
- DevSecOps
- Cloud IAM

Managed

- Cloud Native Security Services
- Cloud, SaaS Posture and Workload Protection

Retainer

- Secure Cloud Foundations
- X-Force Incident Response
- Post Breach Response

Tailored

- Address customer specific Hybrid Cloud requirements

NIST CSF Alignment

Identify

Protect

Detect, Respond

Recover

Zero Trust for Hybrid Cloud



Identities



Data



Applications



Workloads



Networking



DevSecOps

Hybrid Clouds Secured



Microsoft Azure



vmware

IBM Cloud

Google Cloud

IBM Services Platform



DIGITAL
USER
EXPERIENCE



COMPREHENSIVE
SECURITY
OPERATIONS



DATA
INGESTION &
ENRICHMENT



COGNITIVE
ANALYTICS

Ensure Compliance and Security Posture



Visibility of Compliance

Current state view of multicloud security configuration and compliance posture



Optimized Security Controls

Design and configuration of cloud security controls and remediation activities



Maintain Compliance with Security Regulations

Steady-state monitoring and management of cloud security controls and compliance



**Cloud
Security
Posture Mgmt**



Defining and monitoring of security and compliance controls in your cloud environment is critical to detect and address misconfiguration risk

Key Delivery Activities

Visibility of cloud assets and threats

- Validate your cloud security requirements and use cases
- Align implementation plan with your enterprise compliance obligations
- Discover and facilitate onboarding of your cloud accounts
- Review your integration requirements

Optimized cloud security controls

- Customized configuration and optimization of your cloud security controls
- Design and implement automated remediation activities
- Integration with your IT and security technologies, and processes

Continuous monitoring of safe configuration & compliance drift

- Continuous secure configuration management and compliance reporting
- Provide ongoing policy optimization
- Triage and response assistance to address drifts in your security posture
- Review your network and user activity for anomalous behavior

Deliverables

- Current state review report
- High level solution outline
- Onboard accounts to CSPM solution

- Solution Architecture and Blueprint
- Implementation close-out report
- Configured solution

- Ongoing alert triage and escalation
- Weekly review of security findings and remediation activities
- Monthly review of policy enhancements and auto-remediation activities

1-2 Weeks

2-4 Weeks

Ongoing



Multinational Consumer Electronics



2020



Azure, AWS, GCP



Cloud Security Posture Management

The Client Challenge:

- Multiple compliance obligations to adhere to including PCI, HIPAA, and internal standards
- Expanding to a multi-cloud environment, as well as significant workloads on-premise as well
- Did not typically procure consulting or system integration support for security tooling

The Bottom Line:

Looking to improve visibility and telemetry for its multi-cloud environment, as well as for the growing on-premise and cloud container infrastructure

The IBM Solution:

Showcased delivery capabilities through an enhanced proof of concept with the client

This proof of concept was a high engagement delivery over the course of 7 weeks to operationalize key aspects of the solution

IBM team provided clear and present executive alignment with the CISO, partnering with the vendor as well

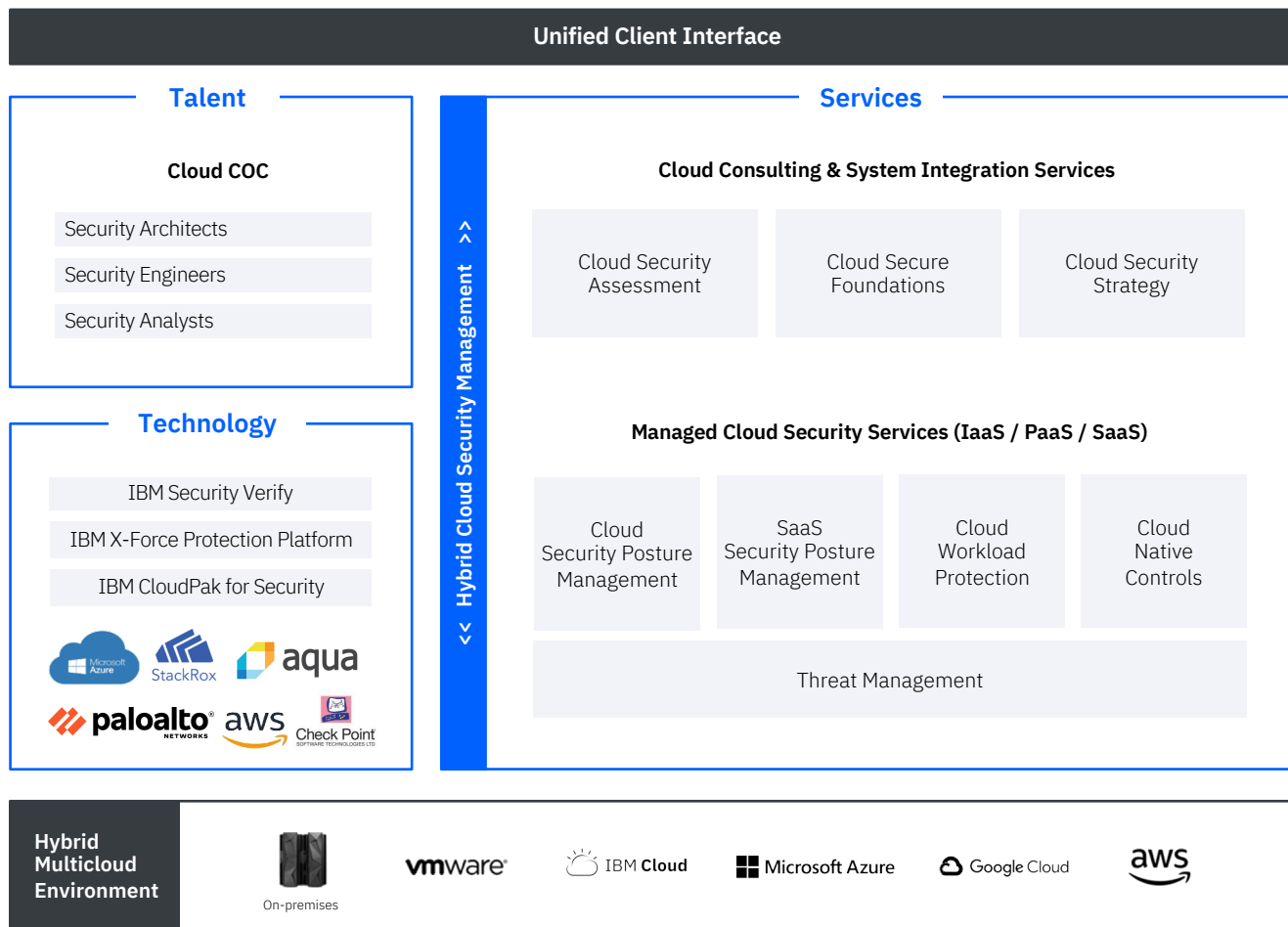
Leveraged IBM Security Research to establish a foundation of through leadership and co-innovation

Delivered implementation and managed services for ongoing steady-state operations

Security Services delivered through a unified experience

Integrated platform
+ best in class tools
+ Real time security insights + Secure environment

- Single Interface
- Insights
- Secure Environment
- Rapid Deployment
- AI based Insights
- Automation



Get to value faster with a strong enterprise cloud security partner

Microsoft
Gold
Consulting
Partner



Microsoft Azure Cloud certified professionals across the globe

- Consulting & Systems Integration
- Managed Security Services
- Solution Design
- Product Management & Engineering



Vendor and cloud agnostic expertise & support

- **Multi-cloud managed security services** providing centralized visibility, management, and monitoring of security operations across hybrid environments.
- Built on an ecosystem of best-of-breed security technologies, spanning **cloud-native & 3rd party**.



Comprehensive support for hybrid multi-cloud

- Leading portfolio of **comprehensive cloud strategy & risk consulting capabilities** coupled with strong security strategy, integration & operations expertise.
- **Recognized by leading analyst firms as leader in MSSP space.** Known for deep cloud relevant innovation and comprehensive threat management services.

Next Steps

1

Take our free Quick
Cloud Security Self-
Assessment

ibm.biz/cloud-sec-maturity

2

Sign up for our deep-
dive Rapid Cloud
Security Assessment

3

Learn more
about our Security
Services for Cloud

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

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

© Copyright IBM Corporation 2022. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty, of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

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.