IBM Security Services for Cloud
Protecting the hybrid multi-cloud

Presenter’s name
Title
Cloud has turned traditional cybersecurity on its head

- **Unanticipated Acceleration to Cloud**
  - Pandemic accelerated change and demand to allow users to access the enterprise from anywhere using any device.

- **Disparate Controls & Decentralized Management**
  - New computing approaches, including Edge & multi-cloud, require robust security platforms that can deploy controls consistently & seamlessly.

- **Regulatory Compliance Churn & Governance**
  - With the migration of workloads to the Cloud, Security, and compliance are top-of-mind across hybrid multi-cloud environments.

- **Growing Attack Surface & Threat Landscape**
  - Growing threats, tools and data inhibit security operations across hybrid environments.

- **99%**
  - 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.

- **½**
  - Of world’s stored data expected to reside in public cloud by 2025.

* Source: Gartner, November 10, 2021.
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
Defining and enforcing security and compliance policies to your cloud workloads regardless of where they are running

**Key Delivery Activities**

**Current State Assessment and Roadmap**
- Assessment of the existing environments to understand cloud workload needs and define proper workload-centric security policies
- Review of VMs, containers or serverless controls
- Define a future-state roadmap according to your risk appetite

**Detailed design of cloud workload architecture**
- Implement and harden cloud workloads based on defined roadmap
- Harden OpenShift native security controls and/or implement 3rd party solutions to better protect your cloud workloads.

**Continuous policy and threat mgmt. & vulnerability ranking**
- Continuously monitor, detect, triage, and respond to security alerts, and threat.
- Automated threat mgmt. using IBM X-Force Protection platform
- Provide/deploy recommendations on policy updates based on app or business needs.
- IBM X-Force Red™ driven vulnerability ranking and prioritization

**Deliverables**

- Current state assessment report with observations, recommendations and roadmap
- Solution and Reference Architecture
- Integration plan and Report
- Vulnerability, runtime and compliance reports

**Cloud Workload Protection**

- 2-4 Weeks
- 4-6 Weeks
- Ongoing
Protect Cloud Workloads

- Current state of Kubernetes and/or OpenShift security controls and application security requirements
- Design & implementation of cloud workload security technologies and policies
- Steady-state management of security policies, vulnerabilities, and threats

Manage & Respond to Container Threats

Review & Remediates Container Vulnerabilities

Free Trial Container Security Dashboard
The Client Challenge:

- Customer provides internal services to multiple customer accounts by leveraging a DevSecOps OpenShift platform
- Provides support for commercial accounts through automating DevOps pipeline controls

The Bottom Line:
Customer met with specific compliance requirements where they needed to get enhanced visibility over their container deployments in order to improve the overall security posture of their enterprise platform

The IBM Solution:

The IBM SSC managed solution helps to enhance the customer’s visibility and protection capabilities across their hybrid cloud container workloads (on-prem and IBM Cloud) on more than 250 worker nodes

Our solution also helped with design, implementation and management of the container security policies based on specific customer compliance requirements

Additional automated threat management capabilities provided that will help detect and respond to any container security events (vulnerabilities, attacks, compliance policies creation, etc.)

Additional Vulnerability Ranking services provided to help detect and prioritize vulnerabilities based on IBM Security’s proprietary algorithm
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

Unified Client Interface

**Talent**

Cloud COC

- Security Architects
- Security Engineers
- Security Analysts

**Technology**

- IBM Security Verify
- IBM X-Force Protection Platform
- IBM CloudPak for Security

**Services**

Cloud Consulting & System Integration Services

- Cloud Security Assessment
- Cloud Secure Foundations
- Cloud Security Strategy

Managed Cloud Security Services (IaaS / PaaS / SaaS)

- Cloud Security Posture Management
- SaaS Security Posture Management
- Cloud Workload Protection
- Cloud Native Controls

Hybrid Cloud Security Management

Threat Management

Hybrid Multicloud Environment

- On-premises
- VMware
- IBM Cloud
- Microsoft Azure
- Google Cloud
- AWS
Get to value faster with a strong enterprise cloud security 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
   <TBD>

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

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.