

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



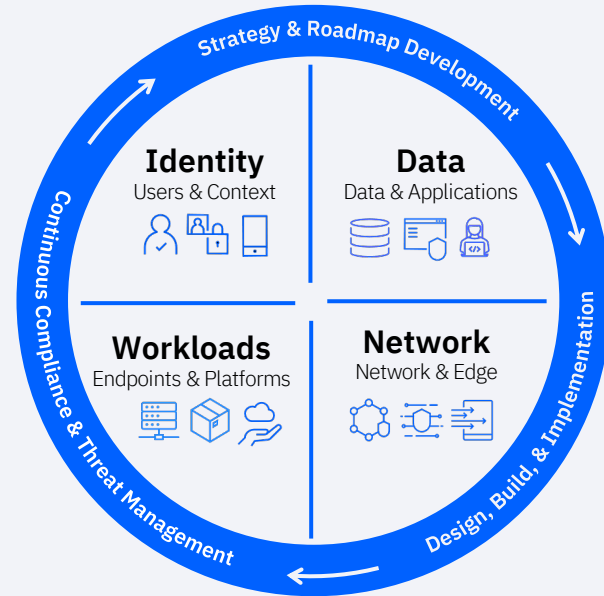
- 02** Enforcing policies to protect cloud resources



- 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

Protect Cloud Workloads



Security Policies Aligned with Acceptable Risk Level

Current state of Kubernetes and/or OpenShift security controls and application security requirements



Protection of Cloud Workloads

Design and implementation of cloud workload security technologies and policies



Continuous Threat Management

Steady-state management of security policies, vulnerabilities and threats



Cloud Workload Protection



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

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

The screenshot shows the Resilient Security console interface. It displays an incident analysis for a container threat. The incident is titled "A CI/Office handle-160116442701 of high magnitude was triggered from 10.0.0.11 targeting with 'Container Security Violation by Twistlock'". The console shows details such as the MSIS Client Name (Name Sample Co), MSIS Client ID (CID0704957), and the Date Created (11/11/2020 19:01). The incident status is "Active" and the severity is "High". The console also shows a list of tasks and a table of incident details.

Review & Remediate Container Vulnerabilities

The screenshot shows the X-Force Red console interface displaying a list of container vulnerabilities. The table includes columns for VID, VULN TYPE, TITLE, CVE Count, WIX, OPPORTUNE, SEV, CVSS BASE, HOST COUNT, OPEN, CLOSED, KR1 SEV, and CATEGORY. The table lists several vulnerabilities, including Microsoft SMB Server Remote Code Execution, Microsoft Windows Remote Privilege, and Microsoft Windows SMBv3 and NFS.

VID	VULN TYPE	TITLE	CVE Count	WIX	OPPORTUNE	SEV	CVSS BASE	HOST COUNT	OPEN	CLOSED	KR1 SEV	CATEGORY
91345	Vuln	Microsoft SMB Server Remote Code Execution	55	0	5	9.3	3	0	3		CRITICAL	Windows
91359	Vuln	Microsoft Windows Remote Privilege	6	95	0	5	9.3	6	0	6	CRITICAL	Windows
91360	Vuln	Microsoft Windows SMBv3 and NFS	6	95	0	5	9.3	6	0	6	CRITICAL	Windows
91361	Vuln	Microsoft Windows Remote Code Execution	6	95	0	5	9.3	6	0	6	CRITICAL	Windows
91338	Vuln	Microsoft Windows Multiple Remote Code	30	32	0	4	9.3	1	0	1	CRITICAL	Windows
91397	Vuln	Microsoft Windows SPIN3 Remote Code	2	21	0	5	9.3	6	0	6	CRITICAL	Windows
90987	Vuln	Microsoft Windows DLL Remote Code Execution	16	0	4	9.3	2	0	2		CRITICAL	Windows
91085	Vuln	Microsoft Graphics Compression Remote	16	14	0	5	9.3	85	3	82	CRITICAL	Windows
370477	Vuln	Apple iTunes Privilege 12.6.2 Multiple Memory	23	13	0	4	9.3	17	0	17	CRITICAL	Local

Free Trial Container Security Dashboard

The screenshot shows the IBM Security Services Cloud Container Dashboard. It displays key metrics for your environment, including Container Vulnerabilities (10), Host Vulnerabilities (1), Container Compliance Issues (62), and Host Compliance (77). The dashboard also features a Security & Compliance Summary section with two donut charts showing Total Security of all Devices (40% compliance) and Total Compliance of all Devices (43% compliance). A sidebar on the right lists various services available for upgrade, such as CI/CD Compliance and Vulnerability Scanning, Vulnerability Prioritization and Ranking, and Runtime Network Protection.





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



Multinational
Technology



2021



IBM Cloud



**Cloud
Workload
Protection**



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

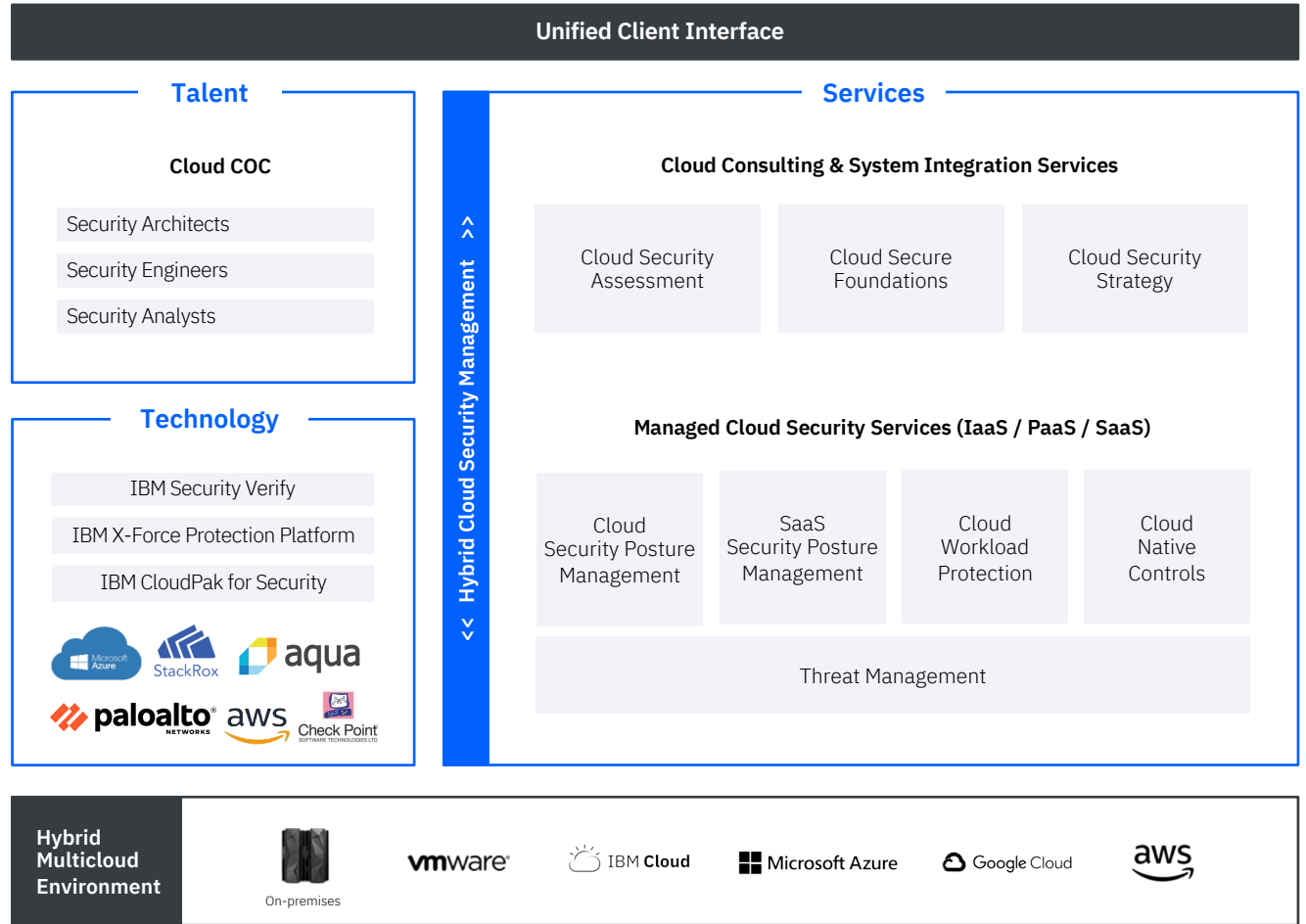
Additional automated threat management capabilities provided that will help detect and respond to any container security events (vulnerabilities, attacks, compliance policies creation, etc.)

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



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

<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

© 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.