Experts Live Kenya

EXPERTS LIVE KENYA

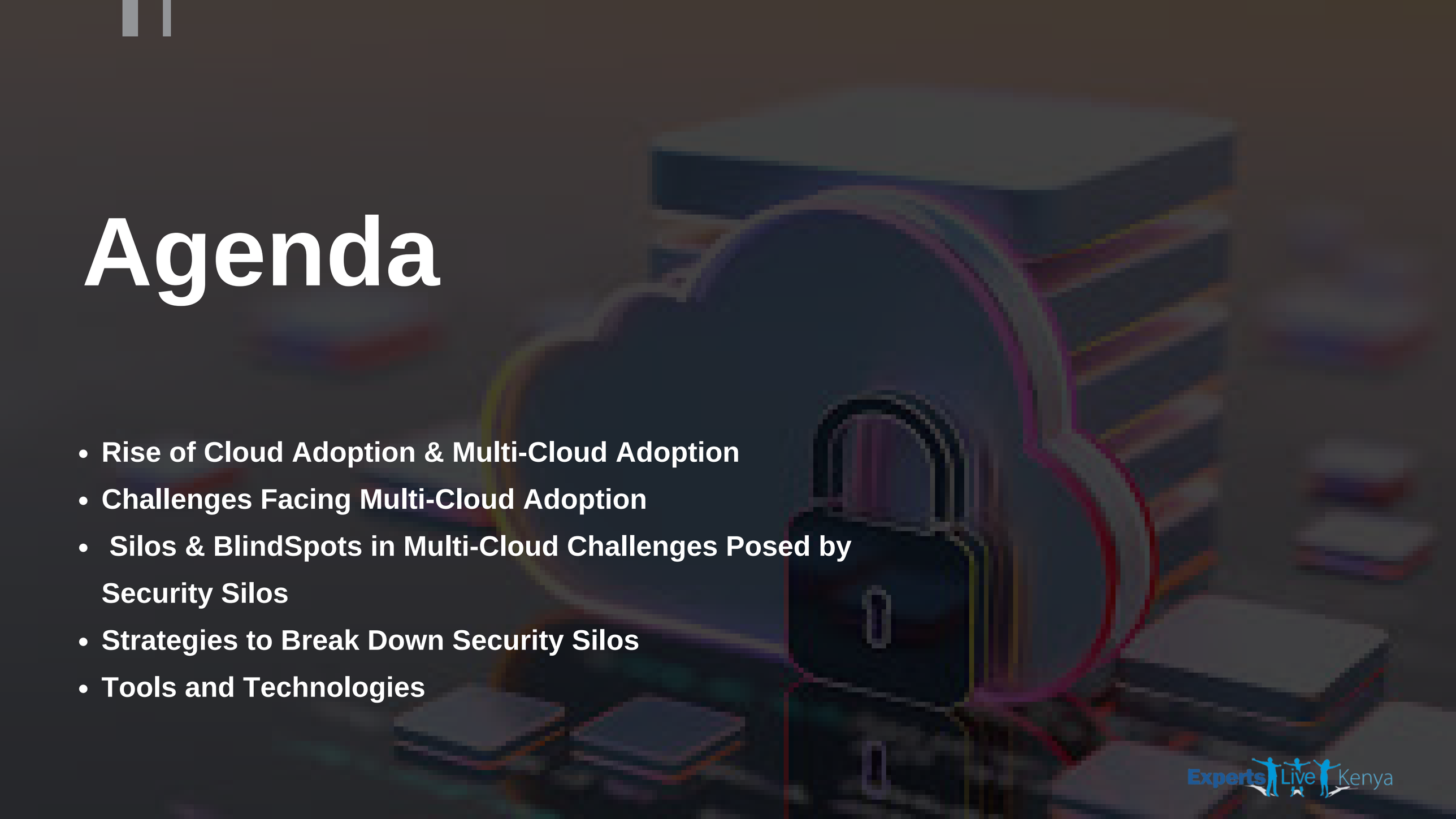
26TH JULY 2024
NAIROBI, KENYA

Experts Live Kenya

Breaking Security Silos Across Your Multi- Cloud Landscape with Microsoft Defender & Microsoft Sentinel

Jacklyne Mbuthia,
Cloud Security Engineer, Cyber Guard Africa

Agenda



- Rise of Cloud Adoption & Multi-Cloud Adoption
- Challenges Facing Multi-Cloud Adoption
- Silos & BlindSpots in Multi-Cloud Challenges Posed by Security Silos
- Strategies to Break Down Security Silos
- Tools and Technologies

ADOPTION OF MULTI-CLOUD

The rise of cloud computing marked the beginning of a new era of innovation, enabling organizations to quickly scale and seize new opportunities. Nowadays, multi-cloud environments have become the standard approach for conducting business.

Approximately 86% of organizations have already adopted a multi cloud approach thanks to its benefits

ADOPTION OF MULTI-CLOUD

A multi-cloud environment refers to the use of multiple cloud computing services from different providers within a single architecture.

Why are businesses distributing workloads across multiple clouds?

- Avoiding Vendor Lock-In
- Optimizing Costs
- Enhancing Resilience and Reliability
- Leveraging Best-of-Breed Services
- Innovation and Agility
- Flexibility and Scalability
- Risk Mitigation

UNDERSTANDING SILOS IN MULTI-CLOUD SECURITY

In multi-cloud environments, silos refer to isolated and disjointed security practices and controls across different cloud platforms. These silos can occur when each cloud provider’s security solutions and policies operate independently of others, creating gaps and inefficiencies in the overall security posture.

Examples of security silos:

- Fragmented Monitoring and Logging
- Inconsistent Incident Response Procedures
- Diverse Security Tools and Technologies
- Isolated Data Protection Measures
- Separate Security Policies

SECURITY SILOS IN MULTI-CLOUD

CHALLENGES

- Identity & Access management
- Complexity
- Inconsistent Security Policies
- Inefficient Threat Response
- Products/technologies to leverage
- Fragmented Visibility
- Securing cloud-native applications and infrastructure throughout the full lifecycle.

VS

STRATEGIES

- Cross-Cloud IAM Solutions
- Unified Security Management
- Consistent Security Policies
- Integrated Monitoring and Logging
- Unified Threat Detection and Response
- Leveraging Multi-Cloud Management Platforms
- Employee Training Programs

TOOLS AND TECHNOLOGIES

FACTORS TO CONSIDER

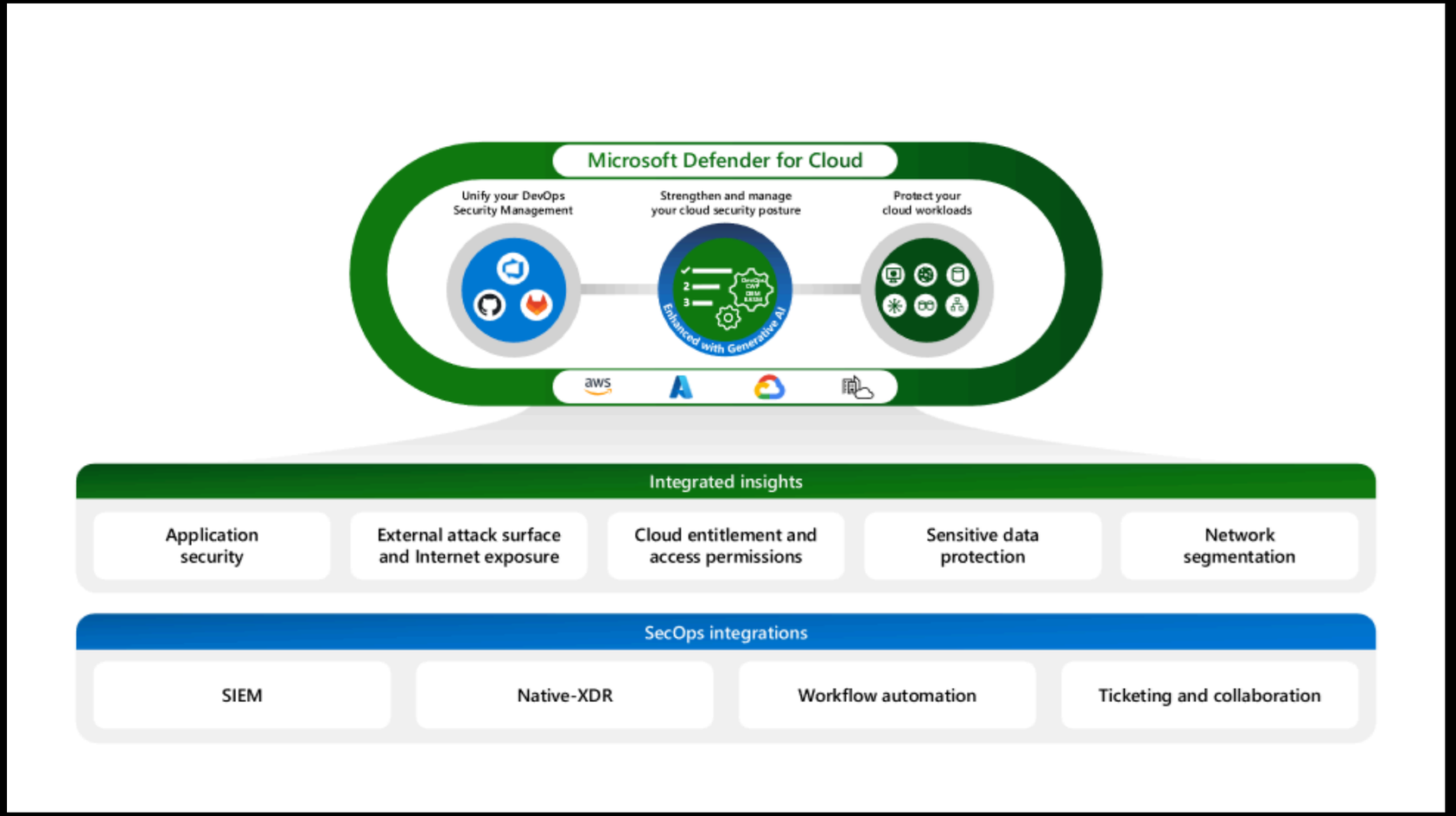
- Integration capabilities
- Scalability
- Automation & Orchestration
- Flexibility & Customization
- User friendliness
- Value for money

VS

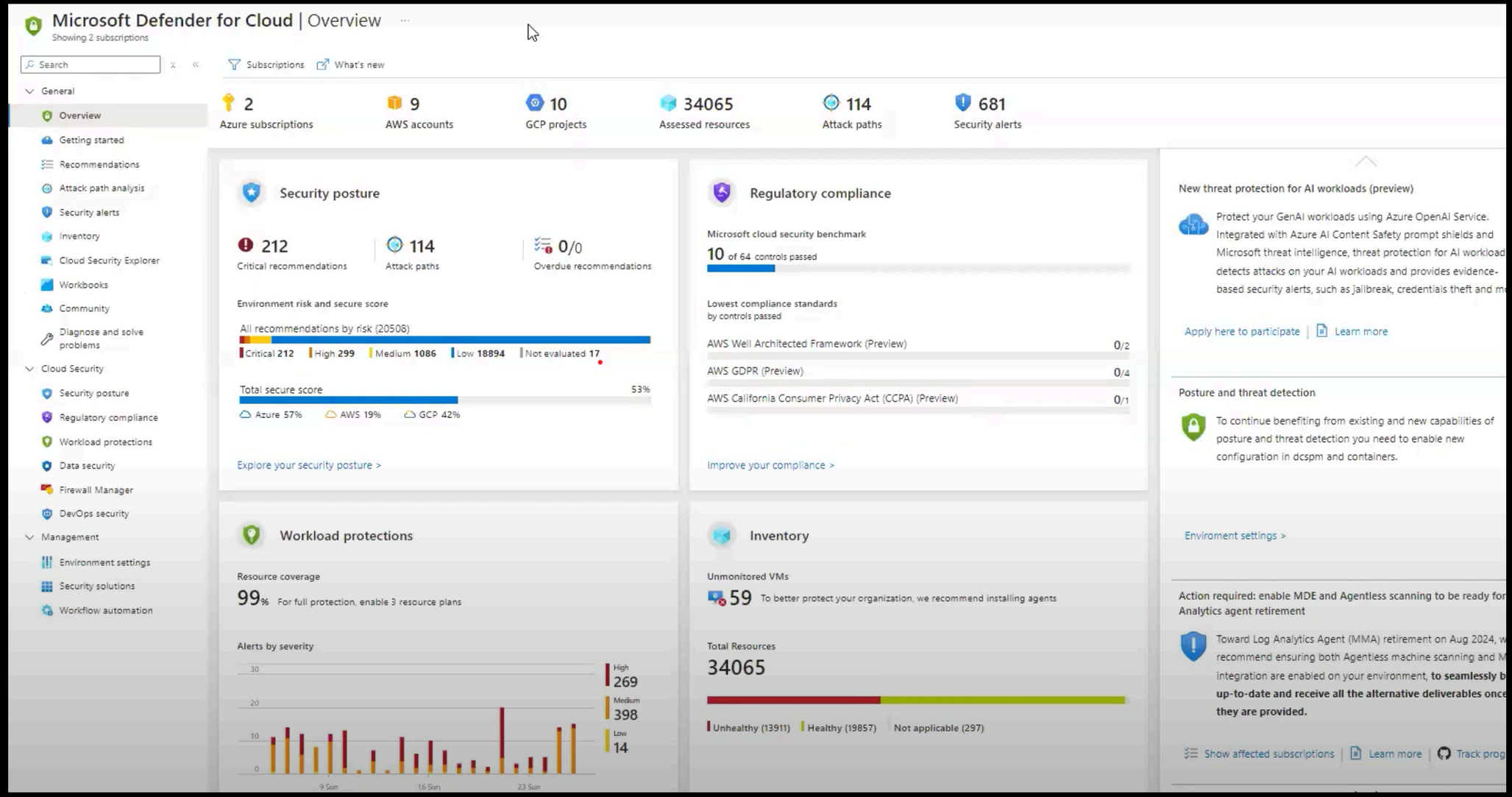
TOOLS TO LEVERAGE

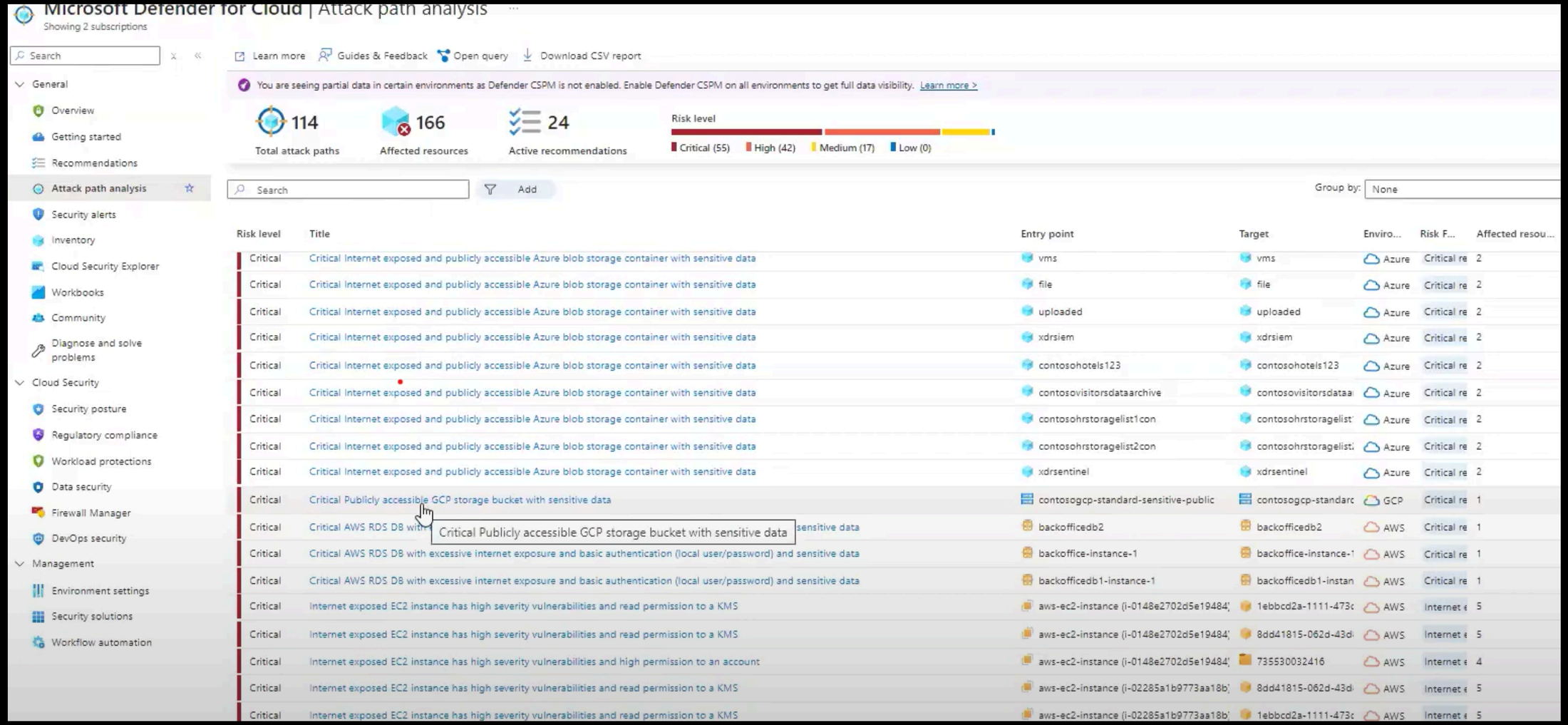
- Security incidents and events managements(SIEM)
- Cloud-native application platform protection (CNAPP)
- Cloud security posture management (CSPM)
- Multi-Cloud Management Platforms

MICROSOFT DEFENDER as MICROSOFT CNAPP SOLUTION

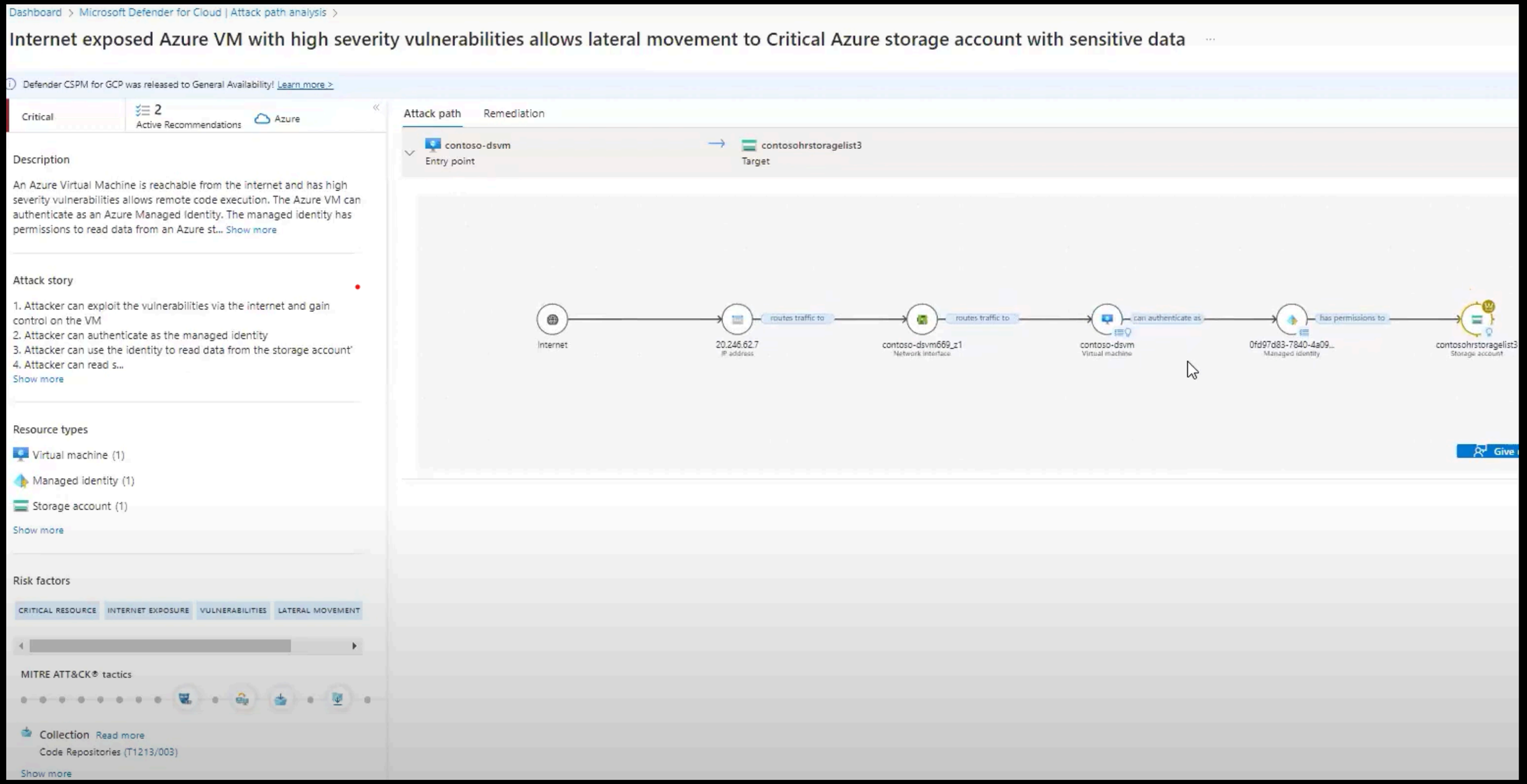


MICROSOFT DEFENDER as MICROSOFT CSPM SOLUTION

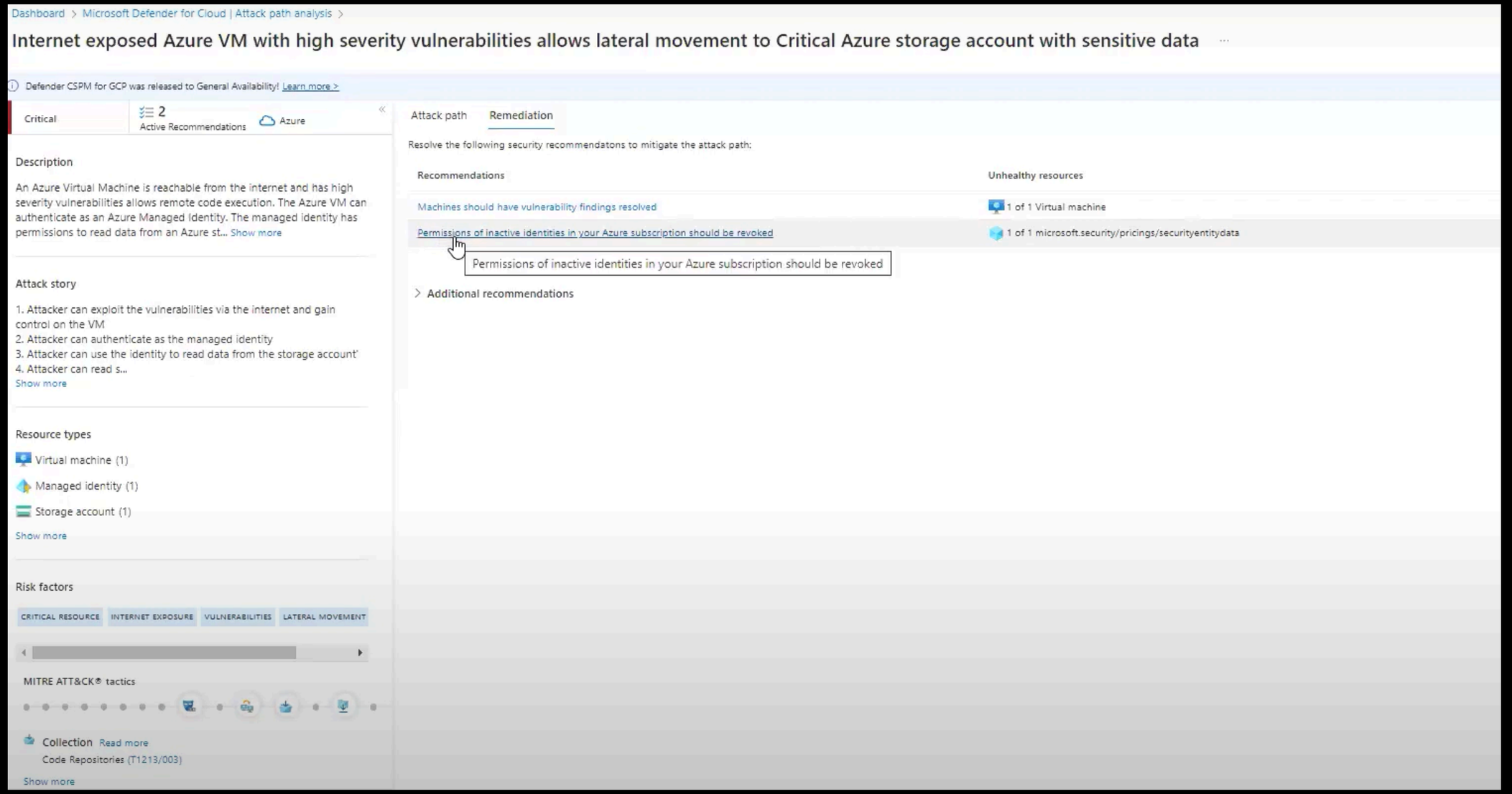




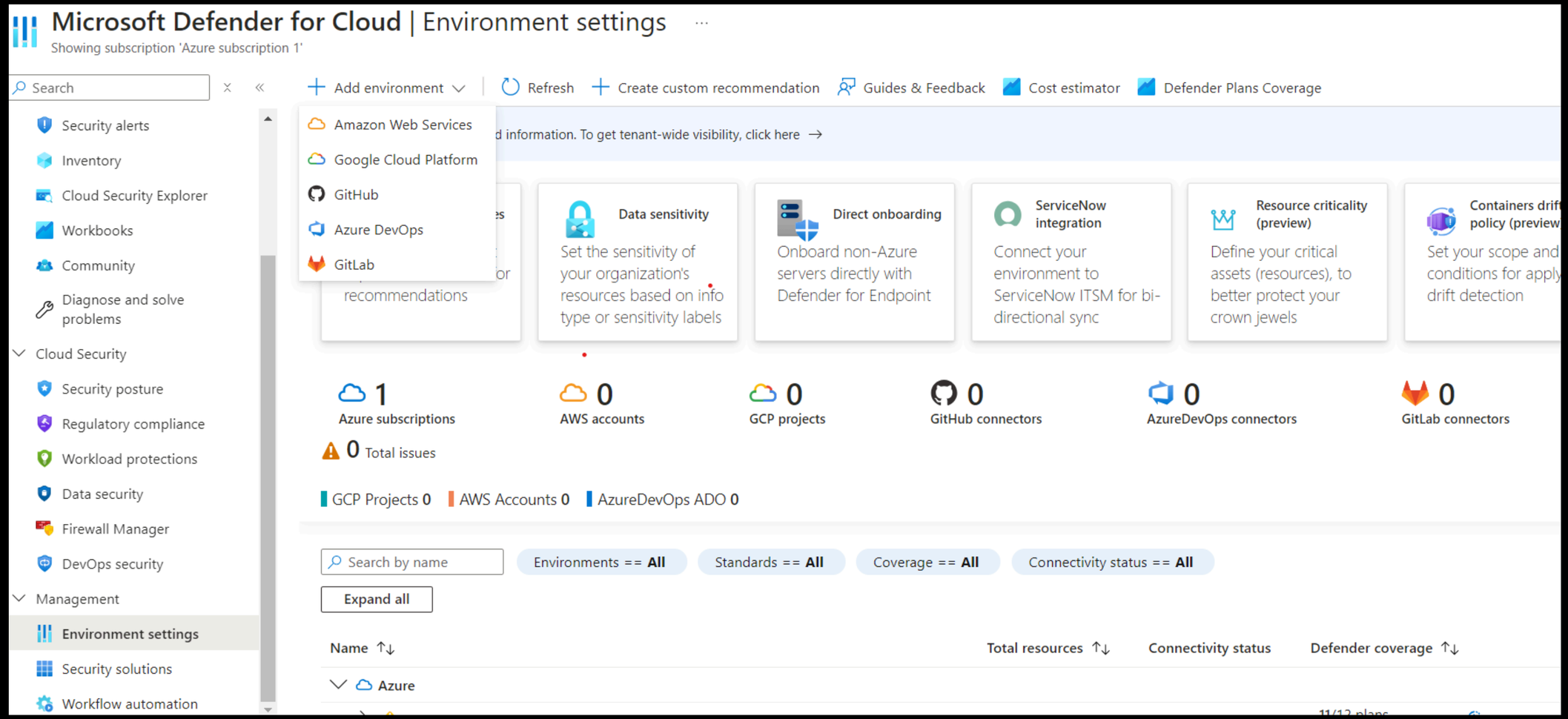
Attack Path analysis is a feature on Defender that allows companies to be able to identify risk in their environment, prioritise how to mitigate them and it's how to refactor it



Attack Path analysis allows you to analyse at a granular level

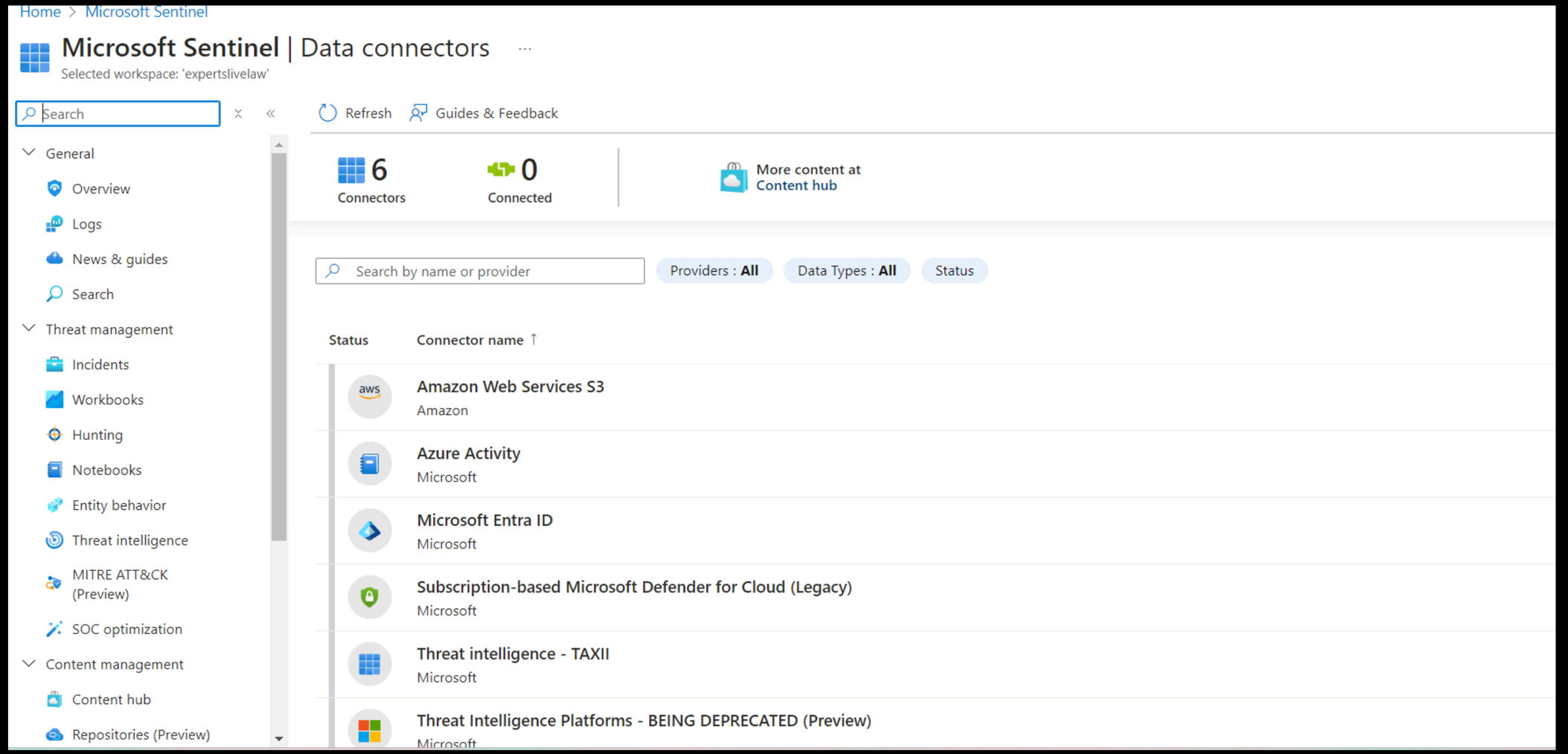


Actionable recommendations are provided for issues identified

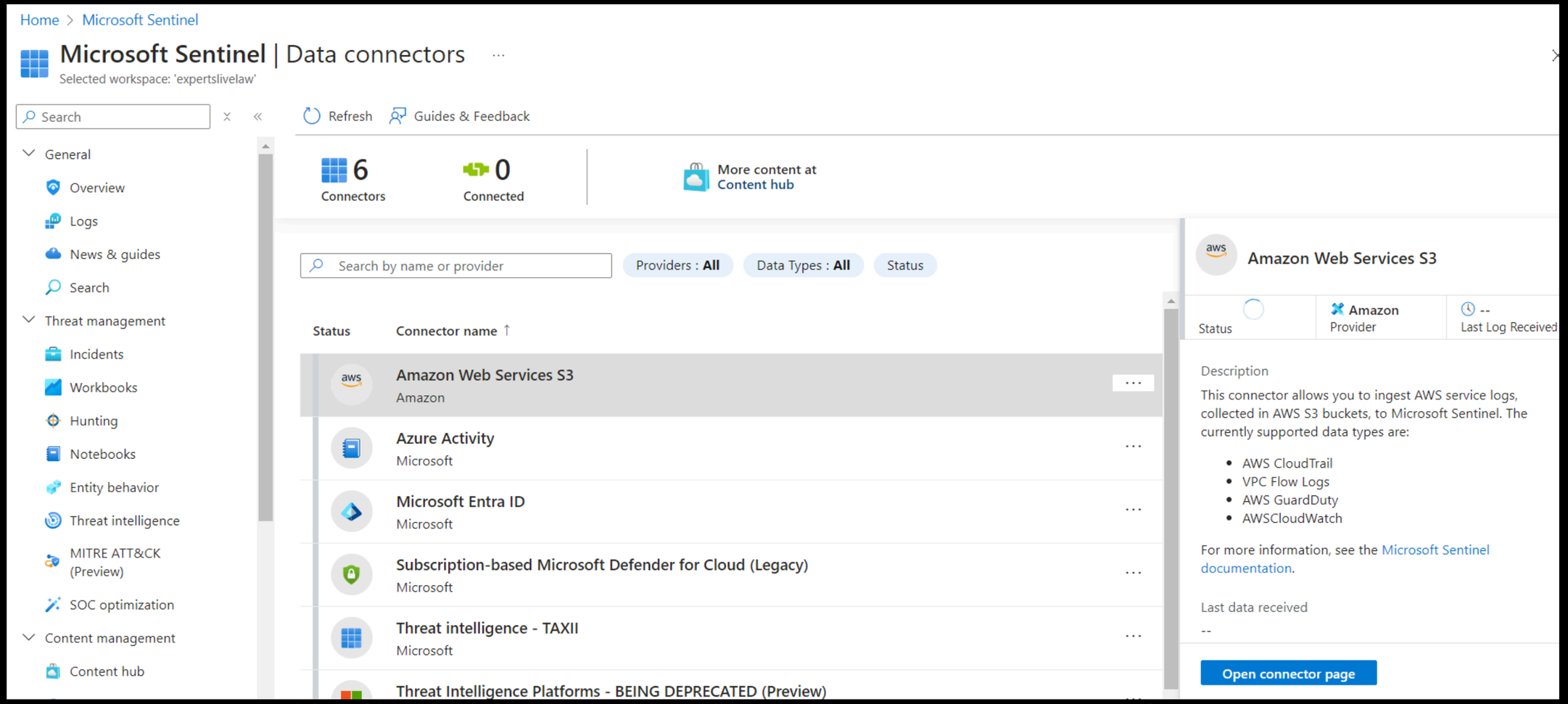


Adding CSPs and developement platforms to Microsoft Defender

MICROSOFT SIEM SOLUTION - MICROSOFT SENTINEL



Sentinel uses data connectors to enable you to integrate to your environments



Identify what the connector will capture to plan out your environment

Conclusion

Multi cloud security is growing, we have to grow in how we are approaching security as well !

Session Feedback

Session Track: Security

Session Name: Breaking Security Silos Across Your Multi- Cloud Landscape with Microsoft Defender & Microsoft Sentinel

Experts Live Kenya

THANK YOU

Speaker Name: Jacklyne Mbuthia

Speaker Title: Seniro Cloud Security Engineer,
Cyber Guard Africa

Speaker Social Media/links:
X: @bugsandbags__

Experts Live Kenya

THANK YOU TO OUR SPONSORS!

NTT DATA

gebeya

Microsoft

FEITIAN
WE BUILD SECURITY

ADC AFRICA DEVELOPMENT CENTER

USIU AFRICA
United States International University-Africa
Education to take you places

2LINKIT

Computer Revolution Africa Group
Technology redefined

NiCE
IT Management Solutions