Microsoft Defender for Cloud

Enhancing Cloud Security

Agenda

Overview of Microsoft Defender for Cloud

Cloud Security Posture Management (CSPM)

Workload Protection

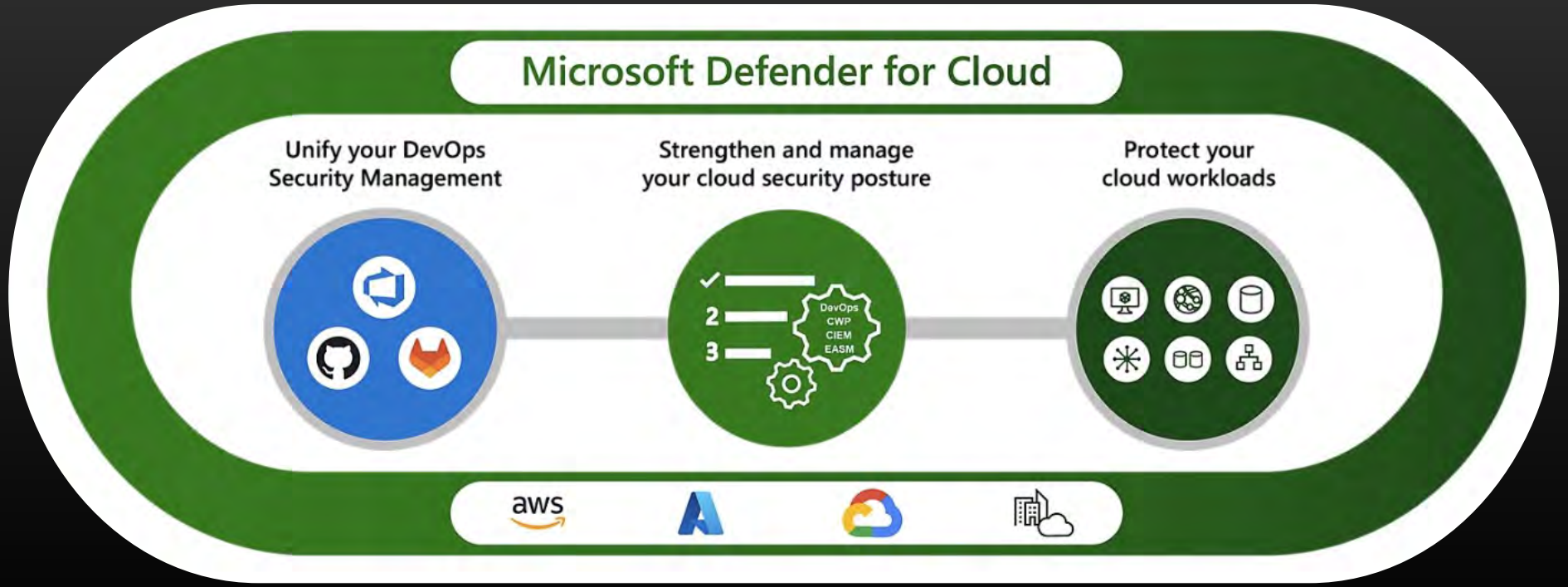
Strengthening Security Posture

User Scenarios and Platform Support

Microsoft Defender for Cloud (MDC)

Cloud Security Posture Management (CSPM)

- Combines several key capabilities
- Enhances overall multi-cloud and on-premise security



Cloud Security Posture Management (CSPM): Hardening Guidance

Recommendations for Security Improvement which is Proactive Security

- Increasing organizational security posture
- Implement effective measures

MDC Visibility

Visibility

- Provides detailed visibility into the security state of your assets and workloads
- Supports Azure, AWS, and GCP and on-premises

Focus on safeguarding critical resources

- Ensuring the security of essential assets
- Implementing measures to protect valuable resources

Workload Protection: Threat Protection

Workload Protection

Guards workloads across multi-cloud environments

Ensures security in hybrid environments

Threat Protection

Provides comprehensive threat protection

Secures against various types of threats

Strengthening Security Posture

Strengthens Security Posture

- Enhances overall security measures

Identifies Weak Spots

- Detects vulnerabilities in the system

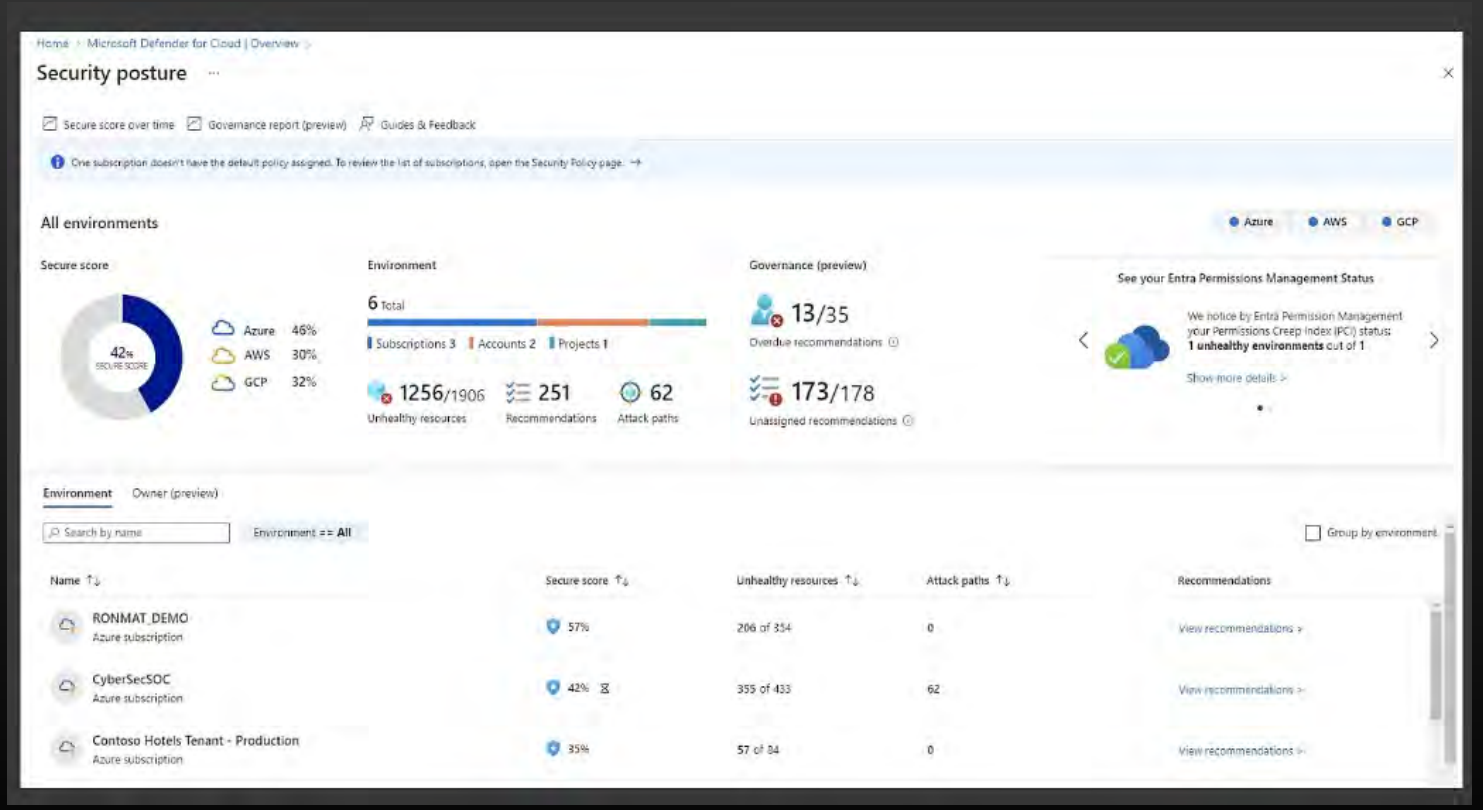
Protects Workloads

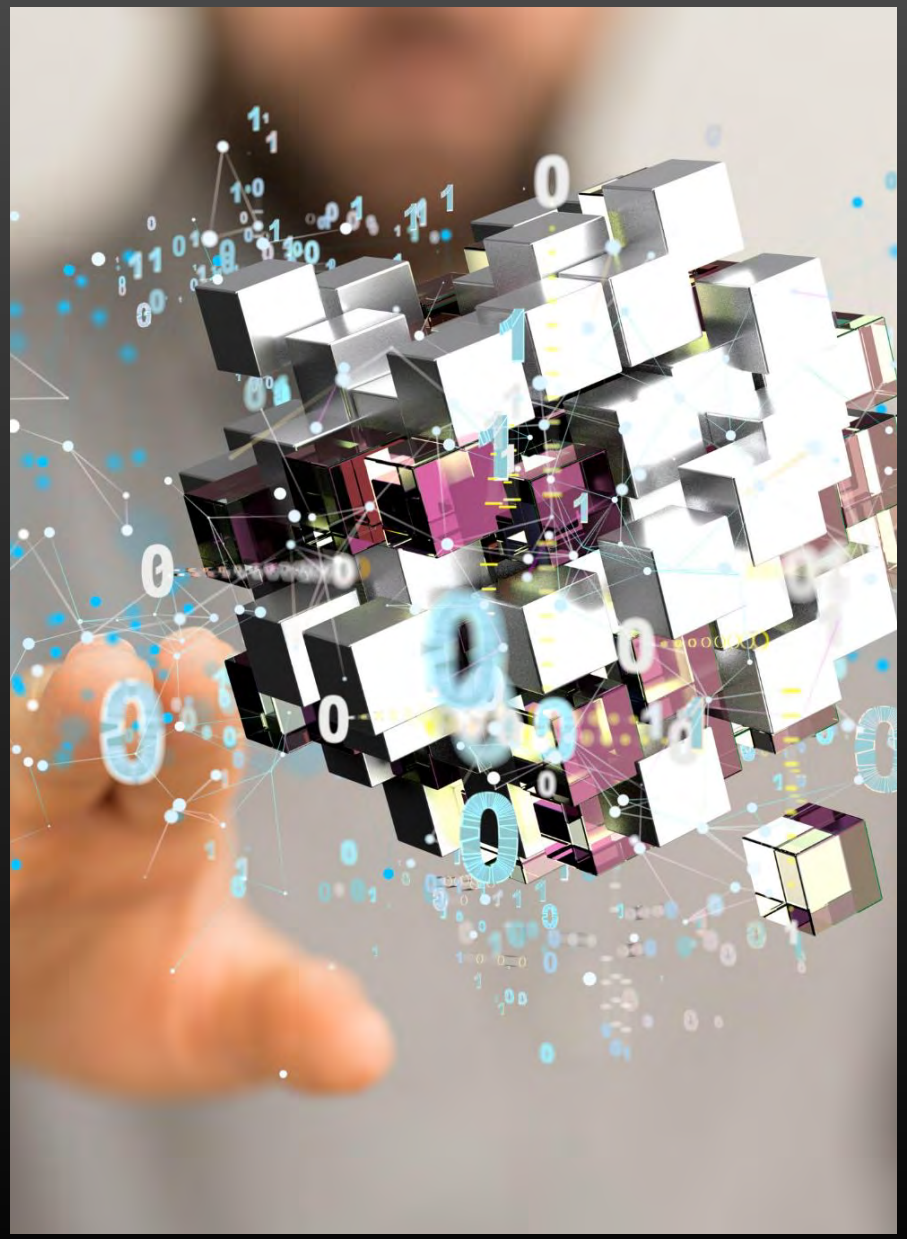
- Safeguards data and applications

CSPM Secure Score

Secure Score Definition

- Aggregates a score based on security benchmarks
- Higher scores indicate lower risk of compromise





CSPM Data Visualization and Reporting

Data Visualization

- Use Azure Workbooks for visualizing data

Reporting

- Generate comprehensive reports using Azure Workbooks

MDC Workflow Automation

Workflow Automation

- Streamlines security tasks
- Reduces manual effort

Benefits of Automation

- Increases efficiency
- Enhances accuracy

Security Tasks

- Automated threat detection
- Automated incident response

CSPM Agentless VM Vulnerability Scanning

Agentless VM Vulnerability Scanning

- Supports Azure, AWS, and GCP
- Scans VMs for vulnerabilities
- Does not require an agent

CSPM Code-to-Cloud Mapping

Code-to-Cloud Mapping

- Maps code to containers
- Maps code to infrastructure-as-code (IaC)
- Enhances security
- Embrace DevSecOps

Workload Protection: DevSecOps Integration and IaC

DevSecOps Integration

- Operates at the code level
  - GITHUB, GitLab, DevOps source code management
- Ensures secure deployment
  - Infrastructure-as-Code (IaC) Security

Secure Coding Practices

- Recommendations for writing secure code
- Guidelines to prevent security vulnerabilities

CSPM Regulatory Compliance Assessments

Purpose of Assessments

- Ensures adherence to standards

Compliance Standards

- Various industry-specific regulations

Assessment Process

- Review of policies and procedures
- Evaluation of practices

Outcome of Assessments

- Identification of compliance gaps
- Recommendations for improvement

CSPM New Data Security Posture Management (DSPM)

Data Security Posture Management (DSPM)

- Scans for sensitive data
- Works with Purview

CSPM: Permissions Management (CIEM)

Permissions Management

- Manages permissions across cloud environments

Conclusion

Unifying DevSecOps Security Management

- Integrates security into DevOps processes

Strengthening Cloud Security Posture

- Provides contextual insights for better security

Protecting Cloud Workloads

- Defends against modern cyberthreats

Hybrid and Multicloud Platforms Supported

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform
- On-premises workloads