Extending Security Visibility Beyond Azure

Hybrid infrastructure, DevOps pipelines, and external attack surfaces

Modern enterprise environments are no longer limited to a single Azure subscription. Workloads run across hybrid infrastructure, applications are built through DevOps pipelines, and exposure exists on the public internet.
This project focuses on how Microsoft Defender for Cloud extends security visibility across all of these areas.

PerparimLabs

Perparim Abdullahu | Microsoft Cloud Architect | Azure Security Architecture | Zero Trust | © PerparimLabs

The Enterprise Reality

- Hybrid & multicloud infrastructure
- CI/CD pipelines
- Internet-facing assets

Security challenges today extend far beyond Azure resources.
Organizations operate hybrid infrastructure, develop applications through pipelines, and expose services publicly.
Security visibility must follow the workload — not stop at the subscription boundary.

PerparimLabs

Why Visibility Must Extend Beyond the Subscription

- Assets exist outside Azure
- Risk appears before deployment
- Exposure happens externally

Many security risks appear before workloads are deployed or outside Azure entirely. Architects must design security strategies that provide visibility across infrastructure, code, and external exposure — not just cloud resources.

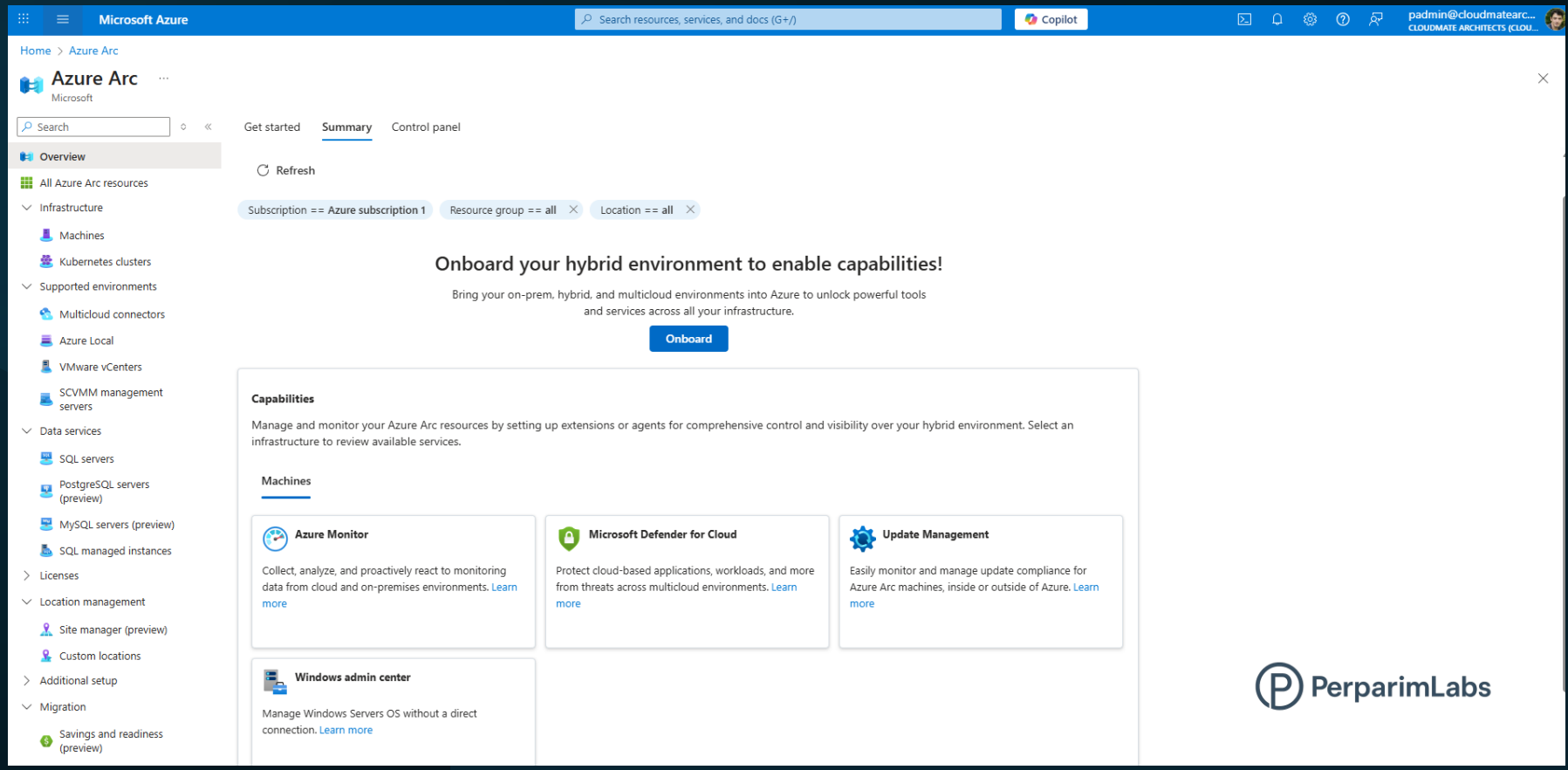
PerparimLabs

Azure Arc: Centralizing Hybrid & Multicloud Visibility

- Single pane of management
- Connect non-Azure resources
- Extend Azure Resource Manager

Azure Arc acts as a bridge between Azure and non-Azure environments.

It allows organizations to onboard servers, Kubernetes clusters, and databases running on-premises or in other clouds, bringing them under Azure Resource Manager for centralized management and security.



PerparimLabs

Azure Arc: Architect Perspective

- Does not move workloads
- Extends governance & security
- Enables consistent policy

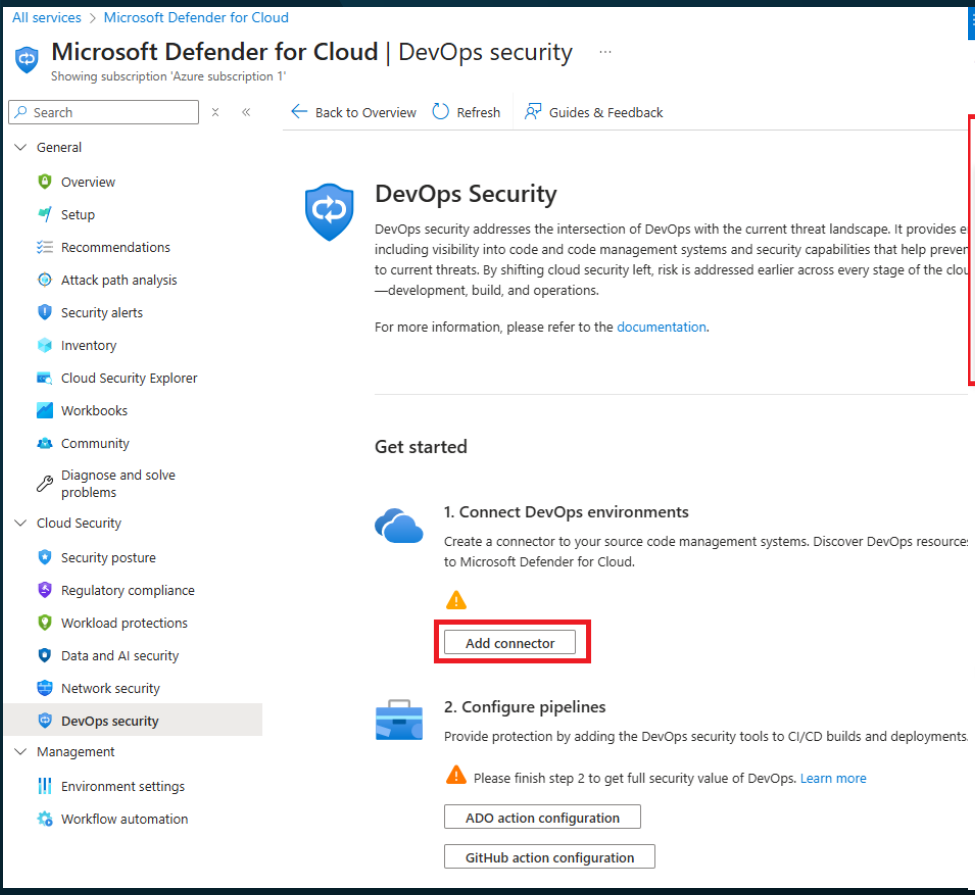
Azure Arc does not migrate workloads into Azure.
Instead, it extends governance, configuration, and security controls to resources wherever they run.
From an architect’s perspective, this provides consistent management across distributed environments.

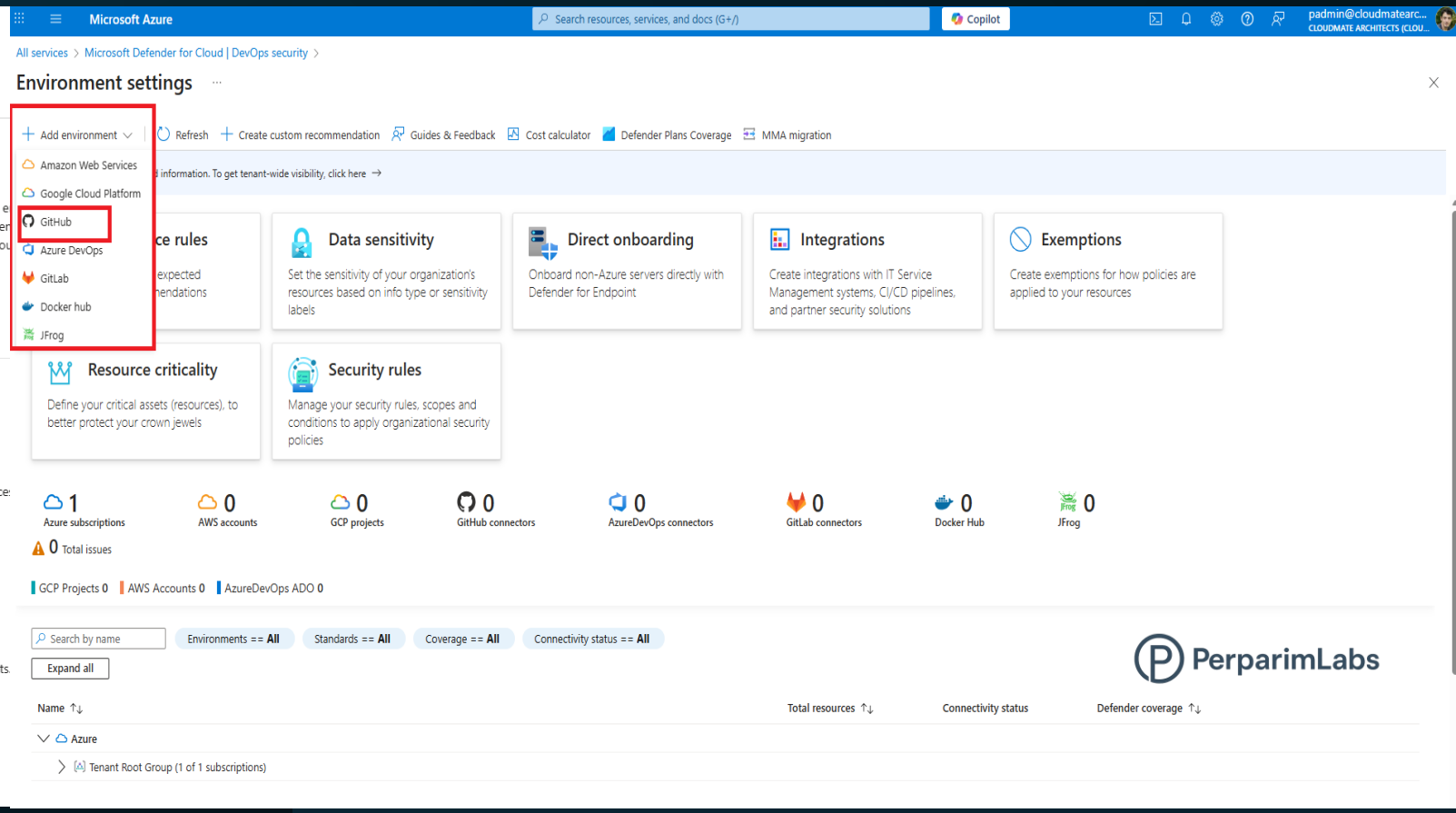
PerparimLabs

Defender for DevOps: Shifting Security Left

- DevOps posture visibility
- CI/CD integration
- Early vulnerability detection

Defender for DevOps focuses on securing the development lifecycle.
By integrating with DevOps platforms such as GitHub, it provides visibility into code vulnerabilities, exposed secrets, and misconfigurations before workloads reach production.





Defender for DevOps: Why It Matters

- Continuous assessment
- Prioritized findings
- Developer-friendly remediation

Security in DevOps is not a one-time scan.
Defender for DevOps continuously evaluates code, prioritizes risk, and helps teams address vulnerabilities early — reducing security debt and production risk.

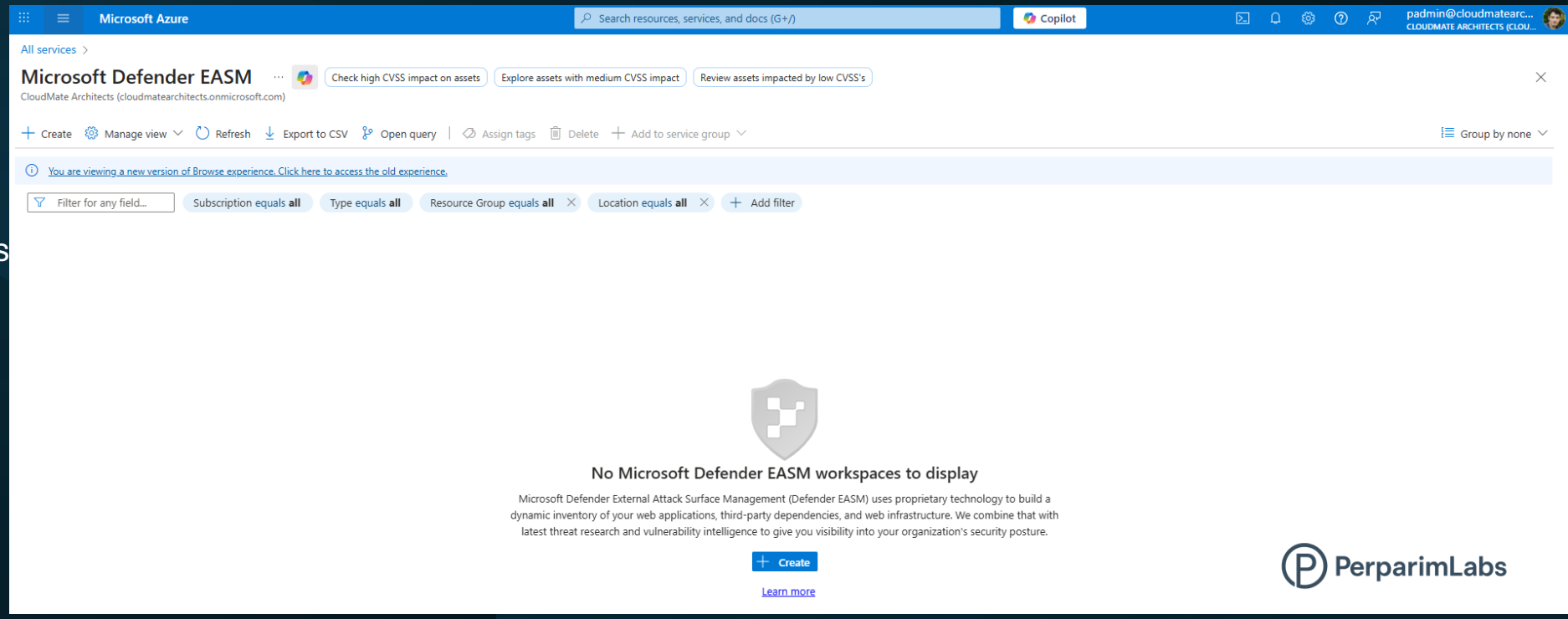
PerparimLabs

Defender External Attack Surface Management (EASM)

- Discover internet-facing assets
- Identify unknown exposure
- Pre-breach visibility

Defender External Attack Surface Management focuses on what exists outside the firewall.

It continuously discovers domains IPs, certificates, and services exposed to the internet, helping organizations understand what attackers can see before a breach occurs.



EASM: External Perspective

- Shadow IT discovery
- CVE & exposure mapping
- External risk context

EASM provides an external perspective of an organization’s digital footprint. This includes shadow IT, forgotten assets, and vulnerabilities that may otherwise go unnoticed by internal security tools.

PerparimLabs

How These Capabilities Work Together

- Azure Arc → Infrastructure visibility
- Defender for DevOps → Code & pipeline visibility
- Defender EASM → External exposure visibility

Together, these capabilities extend Defender for Cloud beyond Azure. Azure Arc secures infrastructure, Defender for DevOps secures pipelines, and Defender EASM reveals external exposure — forming a complete security visibility strategy.

Together, they provide visibility across infrastructure, code, and exposure.

PerparimLabs

Architect Decision Matrix

Area	Capability	Purpose
Hybrid servers	Azure Arc	Centralized management
CI/CD pipelines	Defender for DevOps	Shift-left security
Internet exposure	Defender EASM	External risk discovery

Architects choose these capabilities based on where risk exists.

Each tool addresses a different boundary, together enabling comprehensive visibility.

PerparimLabs

Key Architect Takeaway

Security visibility must follow the workload — not the platform.

Effective cloud security is not limited to Azure resources.
Architects must design visibility across infrastructure, development pipelines, and external exposure to reduce risk at enterprise scale.

PerparimLabs