Enterprise Strategy Group | **Getting to the bigger truth.™**

Technical Validation

Microsoft Defender for Cloud

Protection for Hybrid and Multi-cloud Environments

By Tony Palmer, Principal Validation Analyst

November 2022

This ESG Technical Validation was commissioned by Microsoft and is distributed under license from TechTarget, Inc.

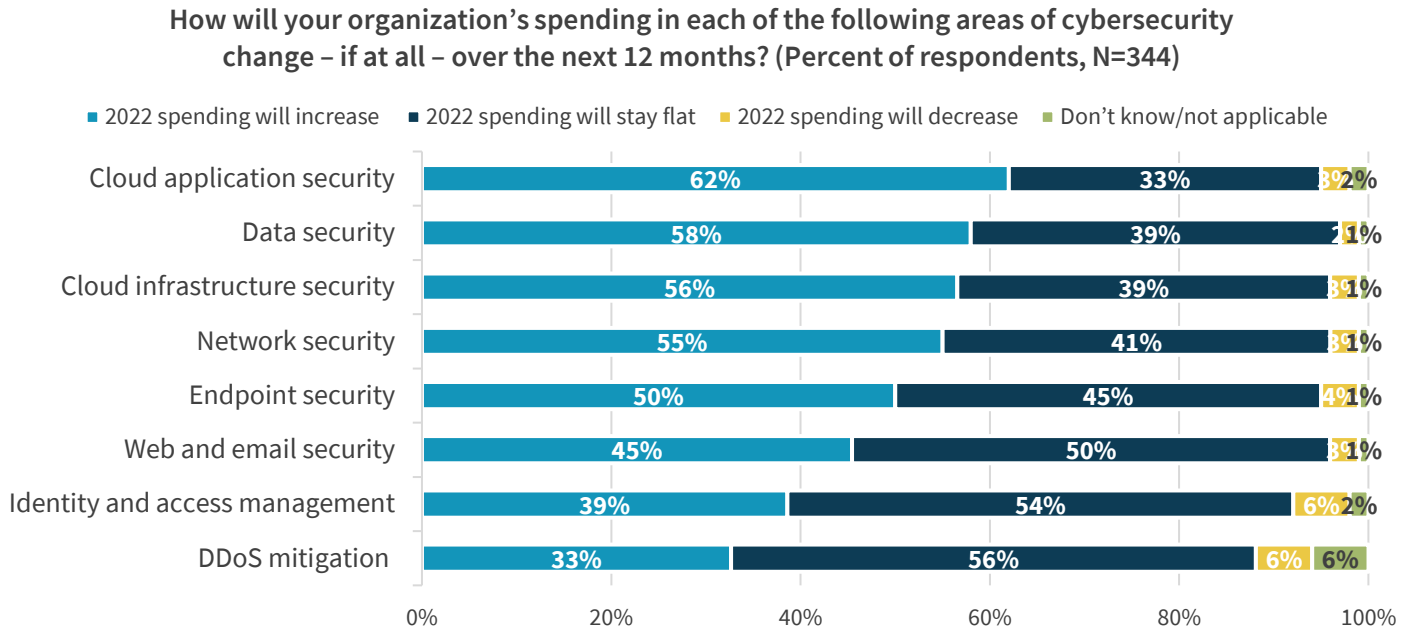
Introduction

This ESG Technical Validation explores Microsoft Defender for Cloud and examines how the solution helps organizations to unify DevOps security management, manage and harden their security posture, detect threats, and protect workloads in hybrid environments and across multiple clouds.

Background

ESG research reveals that organizations aim to address the expanding attack surface with fortified and holistic cybersecurity strategies. According to ESG research, organizations reported that the top cybersecurity areas for planned spending increases in 2022 were cloud and data security, but at least half of organizations also planned to spend more on network security (55%) and endpoint security (50%), which points to the importance of taking a comprehensive approach to cybersecurity (see Figure 1). And given the unabated increase in ransomware attacks and other security threats, it's no surprise that improving cybersecurity was by far the most common criterion for justifying IT investments in 2022.[1]

Figure 1. Cloud and Data Are Top 2022 Cybersecurity Spending Priorities



Source: ESG, a division of TechTarget, Inc.

In addition, the gravity of ransomware attacks makes blocking them a top business priority. More than one-third of organizations (36%) experienced ransomware attacks on at least a monthly basis over the past 12 months, and 48% have been hit by at least one successful attack—with nearly two-thirds of victimized organizations (64%) paying ransoms to the attackers. As a result, more than two-thirds of respondents (68%) said ransomware readiness is of one their organization's top five most important business priorities, with 22% citing it as the top overall business priority. Senior business leadership plays a role in determining ransomware strategy in more than nine out of ten organizations (91%), reinforcing its importance.

[1] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021. All ESG research references and charts in this technical validation are from this research report unless otherwise noted.

Microsoft Defender for Cloud

Microsoft Defender for Cloud is a centralized, integrated cloud-native application protection platform. It is designed to help teams enable security across the development lifecycle, strengthen security posture, and protect multi-cloud workloads against complex threats. Microsoft has introduced advanced plans to enable security across the ecosystem, from development to production: Defender for DevOps, Defender Cloud Posture Security Management, and Cloud Workload Protection capabilities including Defender for Servers, Defender for Storage, Defender for Containers, Database protection, and more.

Figure 2. Microsoft Defender for Cloud Plans

Source: ESG, a division of TechTarget, Inc.

Defender Cloud Security Posture Management (CSPM)

Defender Cloud Security Posture Management (CSPM) is designed to enhance posture visibility, identify and prioritize critical risks, and reduce compliance and governance risk. The combination of agent-based and agentless scanning capabilities provides broad and deep coverage, with agents providing in-depth real-time monitoring and agentless scanning providing the breadth of complete results with no extra resource cost. The intelligent cloud security graph integrates vulnerability management and misconfiguration insights from agentless scanning in multi-cloud servers and multi-cloud containers. Attack path analysis prioritizes the most critical risks based on potential lateral movement paths and risk context. Cloud Security Explorer enables risk hunting by providing admins and power users with templates they can use to find specific types of vulnerabilities, such as vulnerable SQL Server instances exposed to the internet. Additionally, integrated compliance and governance tools enable teams to meet and audit regulatory compliance standards and automate security governance (managing both ownership and progress) at scale.

Secure Score is designed to give organizations a unified view of the security posture of all their clouds, with prioritized security recommendations and the ability to track and manage security posture state over time. Workload-specific signals and threat alerts, leveraging a combination of deterministic-, AI-, and anomaly-based detection mechanisms, as well as Microsoft Threat Intelligence—with 24 trillion signals daily—all work together to protect organizations from existing and zero-day advanced threats.

Defender for DevOps

Defender for DevOps is designed to secure the developer workflow from end to end and unify DevOps security management. With Defender for DevOps, organizations can detect and correct security and quality issues as early as possible in the development cycle, while preventing vulnerabilities from reaching production. To accomplish this, security

teams build connectors with DevOps environments, enable full visibility into the DevOps security posture of application code and cloud resource configurations, integrate deep insights from native application security solutions on Azure DevOps (ADO) and GitHub, and manage DevOps security across multi-pipeline and multi-cloud environments in a single console. Defender for DevOps scans across code, dependencies, and secrets to provide insights and recommendations. It also scans infrastructure-as-code templates and container images to prevent misconfiguration. Both development and security teams have visibility into Defender's reports, increasing collaboration and securing the development lifecycle from start to finish.

Cloud Workload Protection Capabilities

Microsoft Defender for Cloud's Cloud Workload Protection (CWP) capabilities offer centralized management of threats across hybrid and multi-cloud environments by continuously scanning workloads to find and manage vulnerabilities. CWP applies threat protection to new workloads automatically and integrates with Security Information and Event Management (SIEM) systems like Microsoft Sentinel for incident management. It uses Microsoft Threat Intelligence to analyze queries, identify potential brute force attacks, and detect anomalies that indicate access from suspicious IP addresses. CWP reduces an organization's attack surface by scanning compute, service layer, and storage workloads across clouds and offering help to remediate and respond to potential attacks.

Defender for Cloud has a diverse selection of plans, covering servers, containers, databases, storage, applications, Key Vault, ARM, and DNS. Plans and pricing are transparent and public.[2]

Microsoft Defender for Cloud is built into the resource provisioning process with Azure, so no agent deployment is required; users just enable it. Multi-cloud support is provided with agentless onboarding for AWS and Google Cloud Platform posture management with auto-provisioning of new resources, and hybrid environments can take advantage of on-premises resource onboarding with Azure Arc.

ESG Technical Validation

ESG examined Microsoft Defender for Cloud's abilities to provide holistic management and hardening of an organization's security posture, detect threats, protect workloads, and let organizations operationalize security.

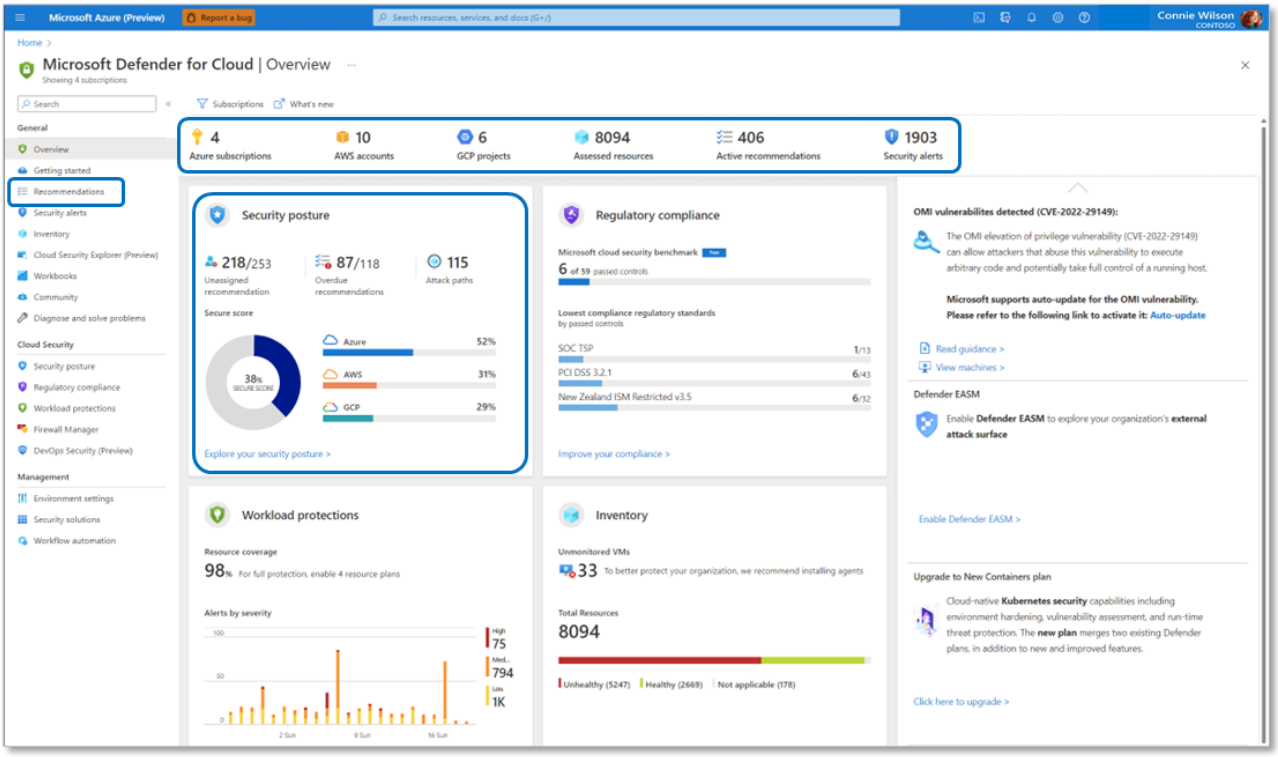
Harden and Manage Security Posture with Defender CSPM

In this section, ESG looks at Defender CSPM and how it helps organizations understand their security postures, implement recommendations based on attack path analysis insights, and monitor the state of their multi-cloud environments over time; how organizations can monitor and manage cloud resource inventories; and how it ensures data security and compliance for organizations, identifying sensitive data and prioritizing critical resources. We then look at how an organization would align with key compliance standards and enforce policies.

First, ESG examined the Defender for Cloud dashboard—the point of entry into the solution. The dashboard provides a high-level overview of the security and compliance status of the whole environment, across all clouds and on-premises resources (see Figure 3). Active Azure subscriptions, AWS accounts, and GCP projects are shown at the top along with a count of the assessed resources, active recommendations, and security alerts.

[2] For more information on Defender for Cloud plans and pricing, visit https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/.

Figure 3. The Microsoft Defender for Cloud Security Dashboard

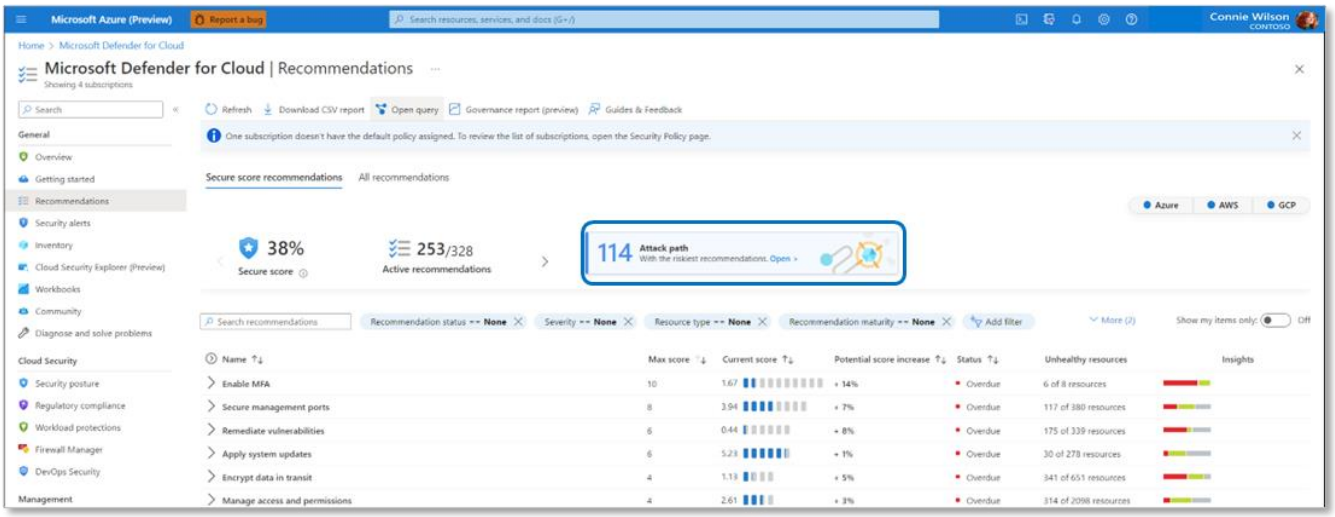


Source: ESG, a division of TechTarget, Inc.

Security posture is a centralized view and tracking mechanism that shows the current security state of all cloud environments. Secure Score, Defender for Cloud's security posture measurement, is calculated by evaluating several categories, including network, access, compute, databases, IoT, app services, and containers. Secure Score projects the score across all resources, whether they are hybrid or multi-cloud, and breaks out individual scores for each CSP.

The dashboard offers insights to help organizations quickly prioritize recommendations, identify their most-attacked resources, and act to protect them. ESG clicked on *Recommendations* to learn more (see Figure 4).

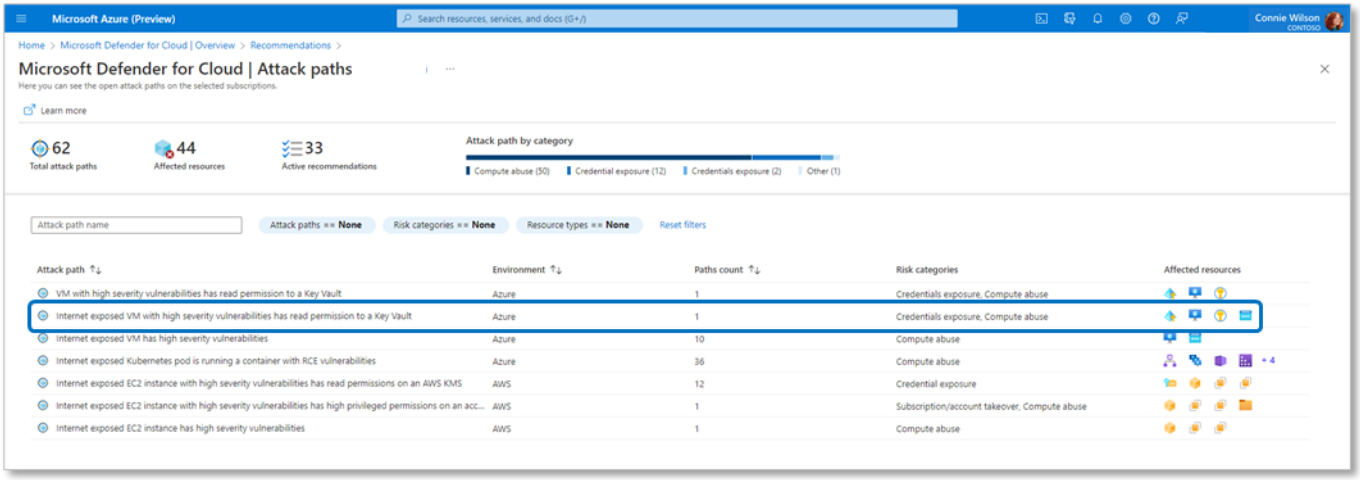
Figure 4. Recommendations



Source: ESG, a division of TechTarget, Inc.

The Recommendations window shows the top issues that should be addressed to improve security posture. A large organization may have hundreds of important recommendations for remediation. The *Attack Paths* view provides insight into which paths should be prioritized. ESG clicked *Attack Paths* to dig deeper. *Attack Paths* provides a unified view of essential risk and vulnerability context across clouds, with detailed descriptions of the vulnerability, the number of paths that contain it, the category of the risk, and the resources affected.

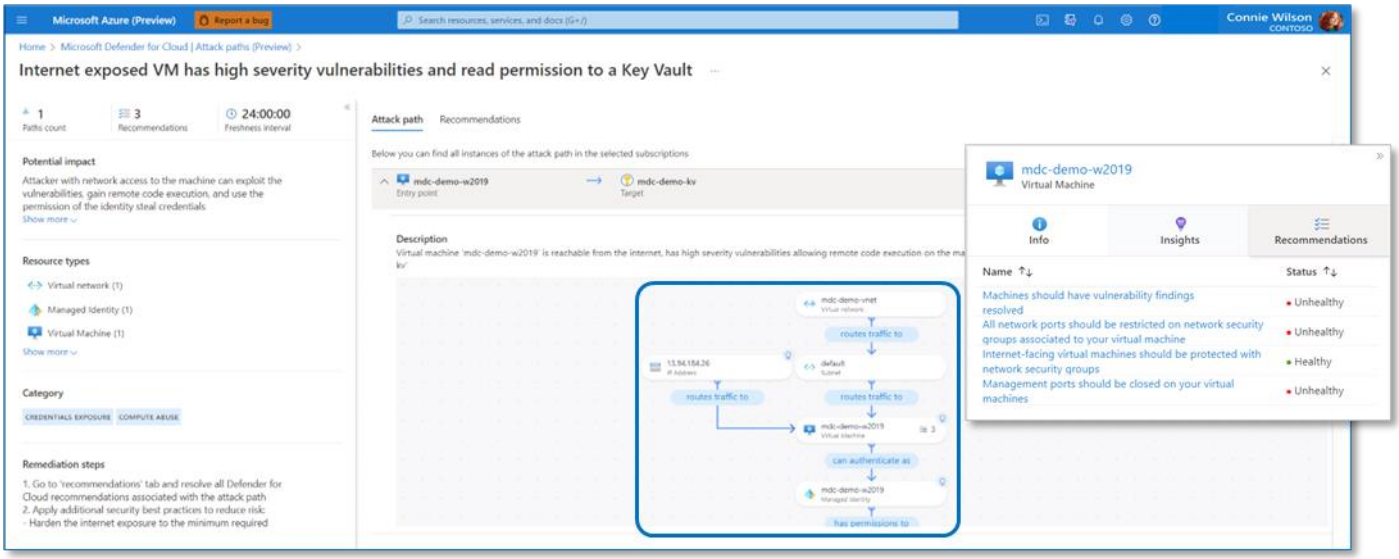
Figure 5. Attack Paths



Source: ESG, a division of TechTarget, Inc.

In this case, Defender identified an internet-exposed VM with permissions to a key vault that has high-security vulnerabilities. Analysts can drill down for more details on the potential impact, the resources and entities involved, and step-by-step recommendations for remediation (see Figure 6).

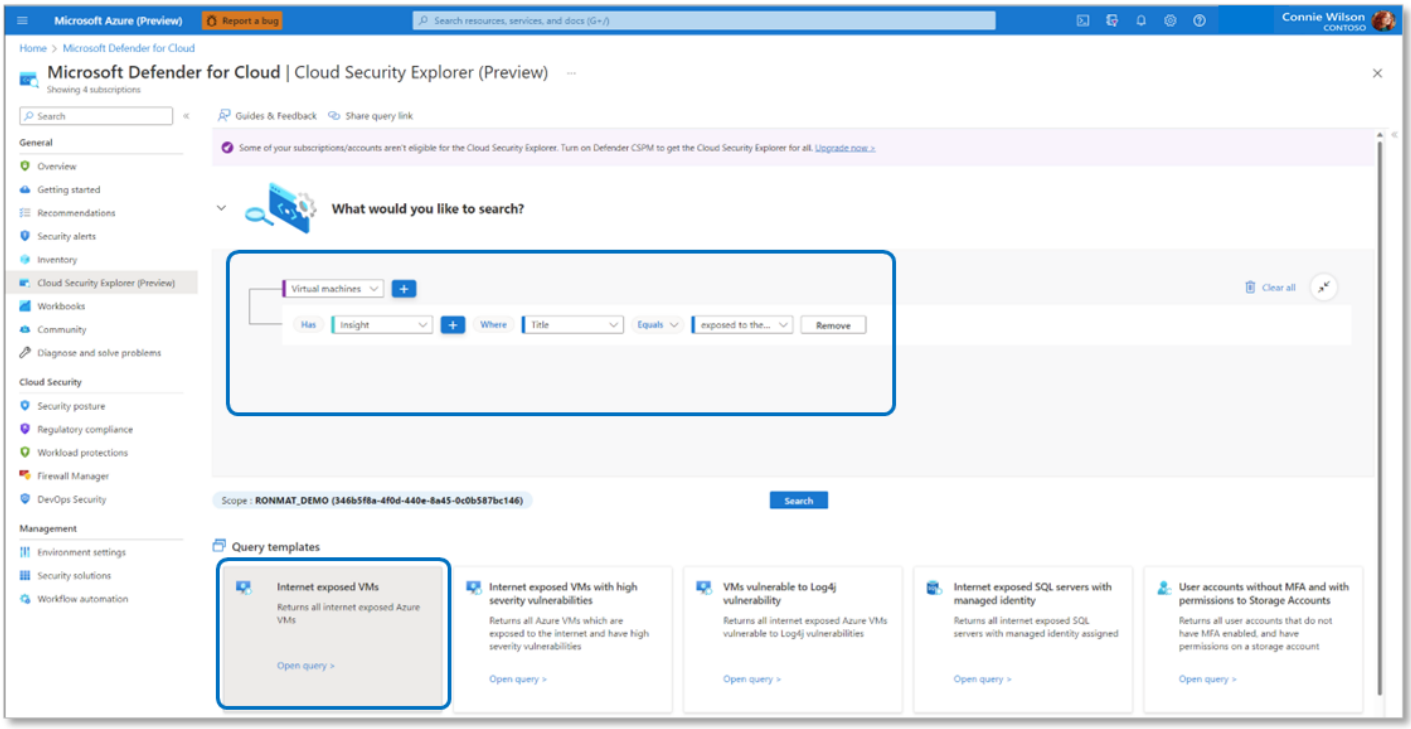
Figure 6. Attack Path Recommendations



Source: ESG, a division of TechTarget, Inc.

The Cloud Security Graph leverages the context engine in Defender for Cloud, allowing graph-based custom queries based on built-in attack paths or created from scratch for issue identification and risk assessment (see Figure 7).

Figure 7. Cloud Security Explorer



Source: ESG, a division of TechTarget, Inc.

This enables security analysts to proactively search for security issues in the environment, including multiple data layers, smart insights, connections, and custom conditions that are relevant for the organization.

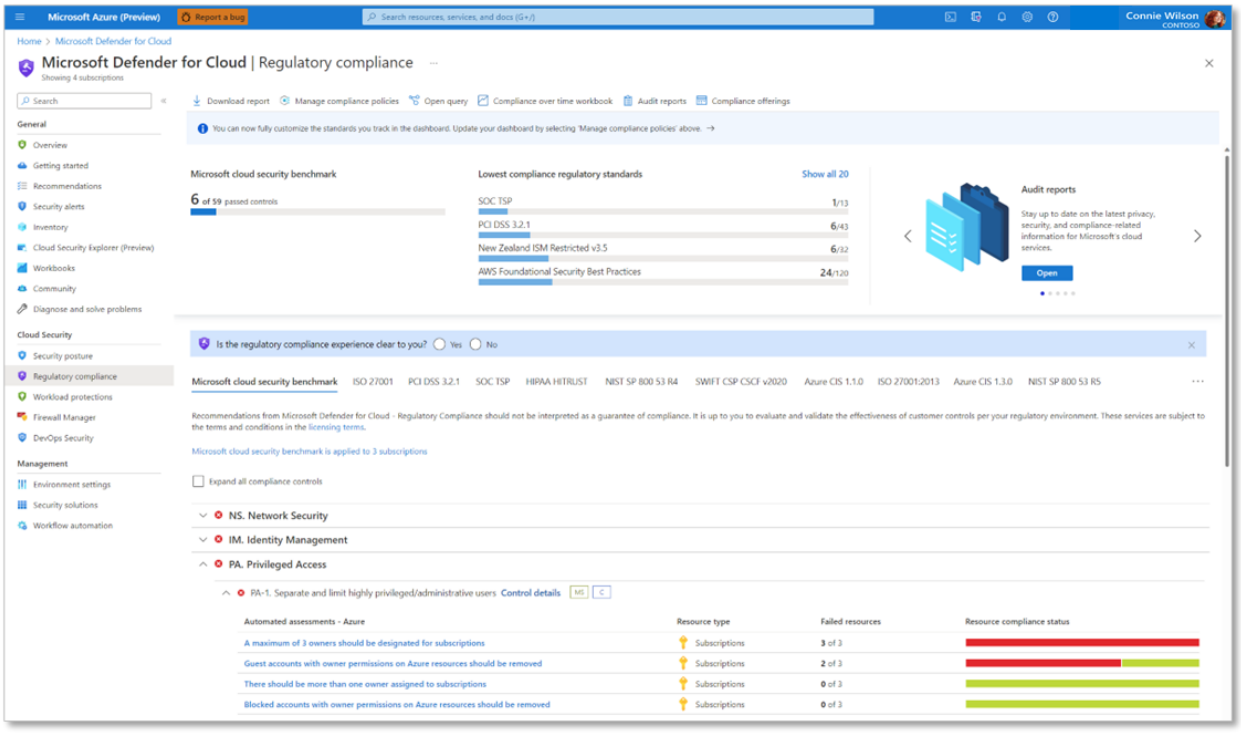
Finally, ESG looked at compliance and governance. Security assessments are mapped to compliance controls and requirements, which enables an aggregated view of compliance status. The Microsoft Cloud Security Benchmark supports all-in-one compliance standards for multi-cloud environments, designed to help customers meet their unique industry standards across clouds. Microsoft attests that this is the industry's first cross-cloud, multiple-standards benchmark.

Microsoft Defender for Cloud's enhanced regulatory compliance capabilities enable customers to audit against their compliance standard of choice with one tool. For example, customers can attach attestation of organizational or operational evidence to meet the full requirements of compliance checks and audits.

The Microsoft Cloud Security Benchmark is monitored in the dashboard by default and is aligned with Secure Score, which means it contains the same set of recommendations. In simple terms, resolving those recommendations helps organizations meet control requirements.

The dashboard is dynamic; an organization can select the precise set of standards that are important to them and customize as needed, allowing organizations to onboard custom standards and define custom control sets. Security Governance functionality is a new built-in feature set in public preview at the time of this writing. Security Governance is designed to set ownership and expected remediation timeframes to resolve recommendations with the goal of further enhancing security posture.

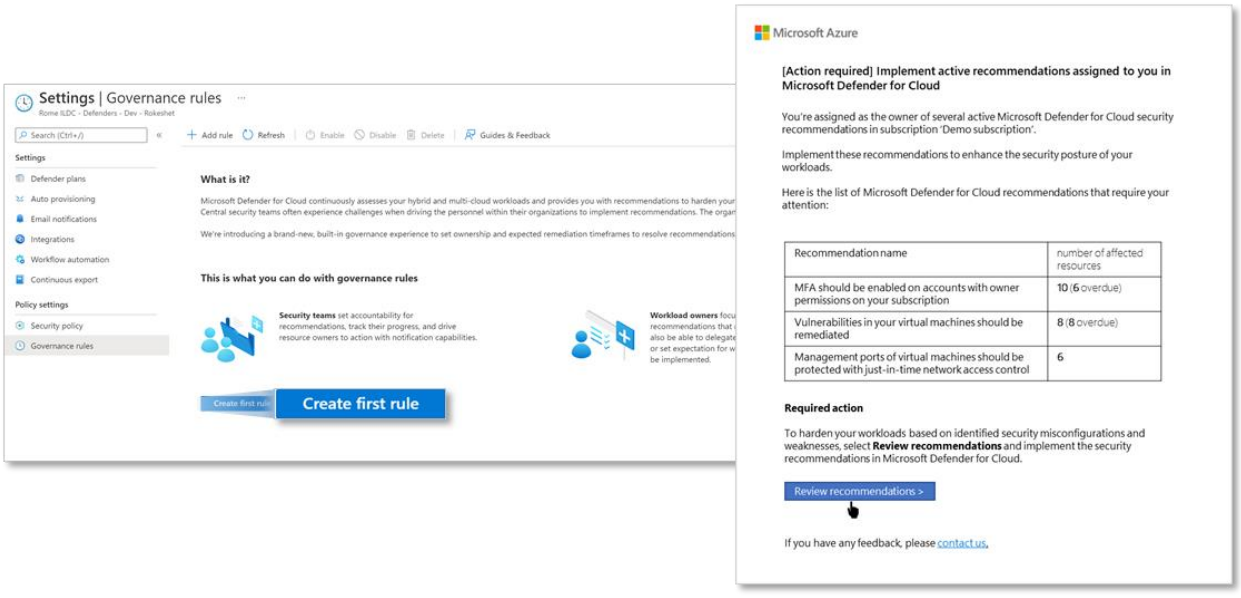
Figure 8. Compliance Monitoring



Source: ESG, a division of TechTarget, Inc.

Security teams set accountability for recommendations, track progress, and drive resource owners to action with notifications. Workload owners focus on the specific recommendations that require their attention and can set expectations for when the recommendations will be implemented or delegate recommendations to others. First, security teams set accountability and the remediation timeframe for recommendations by configuring *Governance rules* at the subscription level (see Figure 9). This triggers an email alerting the resource owner that action is required.

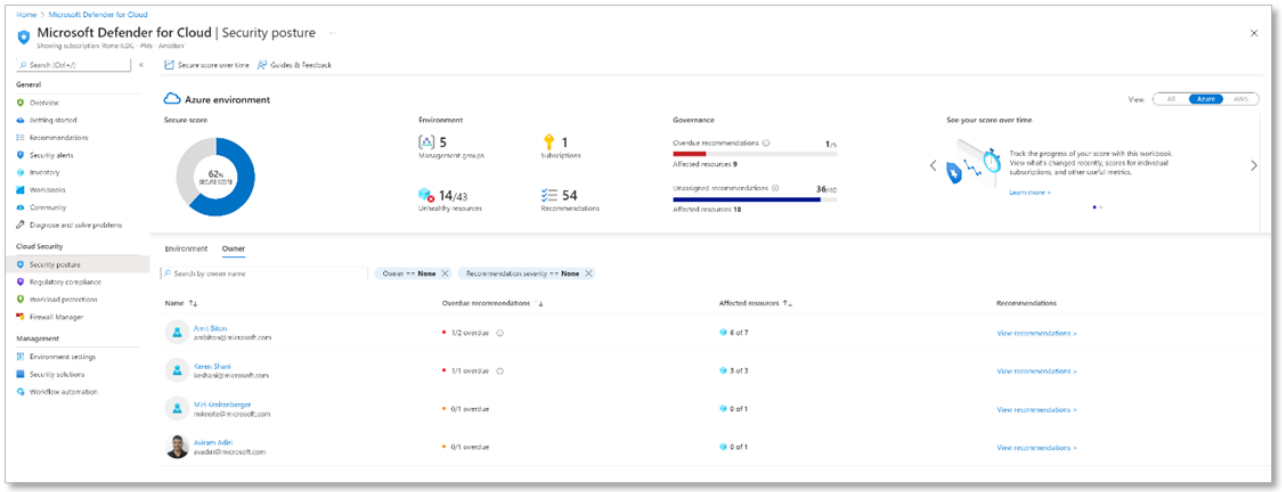
Figure 9. Create a Governance Rule



Source: ESG, a division of TechTarget, Inc.

Owners will receive a summary email weekly with all the recommendations they're assigned to. When there are overdue recommendations, their manager is cc'ed. The *Security posture* page provides visibility into the security status of the entire multi-cloud environment. The *Owner* tab (see Figure 10) displays all owners, with a summary of all recommendations that they're assigned.

Figure 10. Security Posture—Owner



Source: ESG, a division of TechTarget, Inc.

Why This Matters

Almost half (48%) of organizations report a problematic shortage of cybersecurity skills. This ongoing cybersecurity skills shortage has two major implications. The most obvious is a shortage of talented cybersecurity professionals, with simply more cybersecurity job openings than qualified candidates to fill them. The second implication is at least as important: Many members of the current cybersecurity workforce lack the advanced skills necessary to safeguard critical business assets or to counteract sophisticated cyber adversaries. Combine this with the unabated increase in security threats, and security professionals—no matter how qualified—will struggle with an incomplete visualization of what their most urgent risks are.

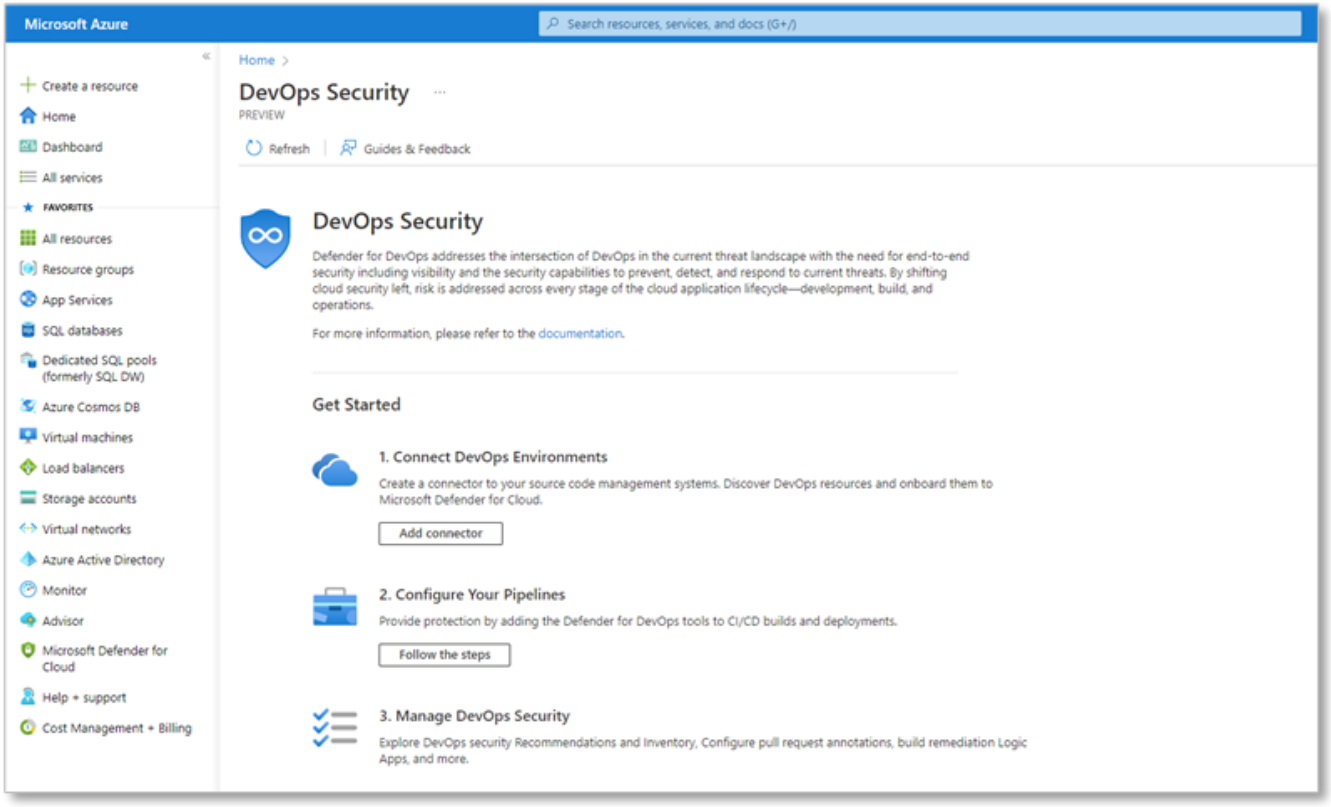
ESG is impressed with the way Microsoft Defender for Cloud identifies and prioritizes vulnerabilities and threats across an organization's cloud configuration. Attack path visualizations and Cloud Security Explorer's easily customizable graph-based queries enable security professionals to focus their attention on what is most important: strengthening the overall security posture of the environment with fast and efficient investigation and response.

Defender for DevOps

ESG examined Defender for DevOps and how it can help organizations to expand and unify visibility, identify and assess risk, and prioritize remediation of threats across all stages of the cloud application lifecycle. Microsoft bundles all the tools needed into a single package that can be easily integrated into workflows with Github and ADO providing shared visibility between development and security teams. Pull request (PR) annotation facilitates communication, enabling coordinated response across development, IT, and security operations teams.

From the Defender for Cloud dashboard, ESG clicked DevOps Security.

Figure 11. DevOps Security—Onboarding

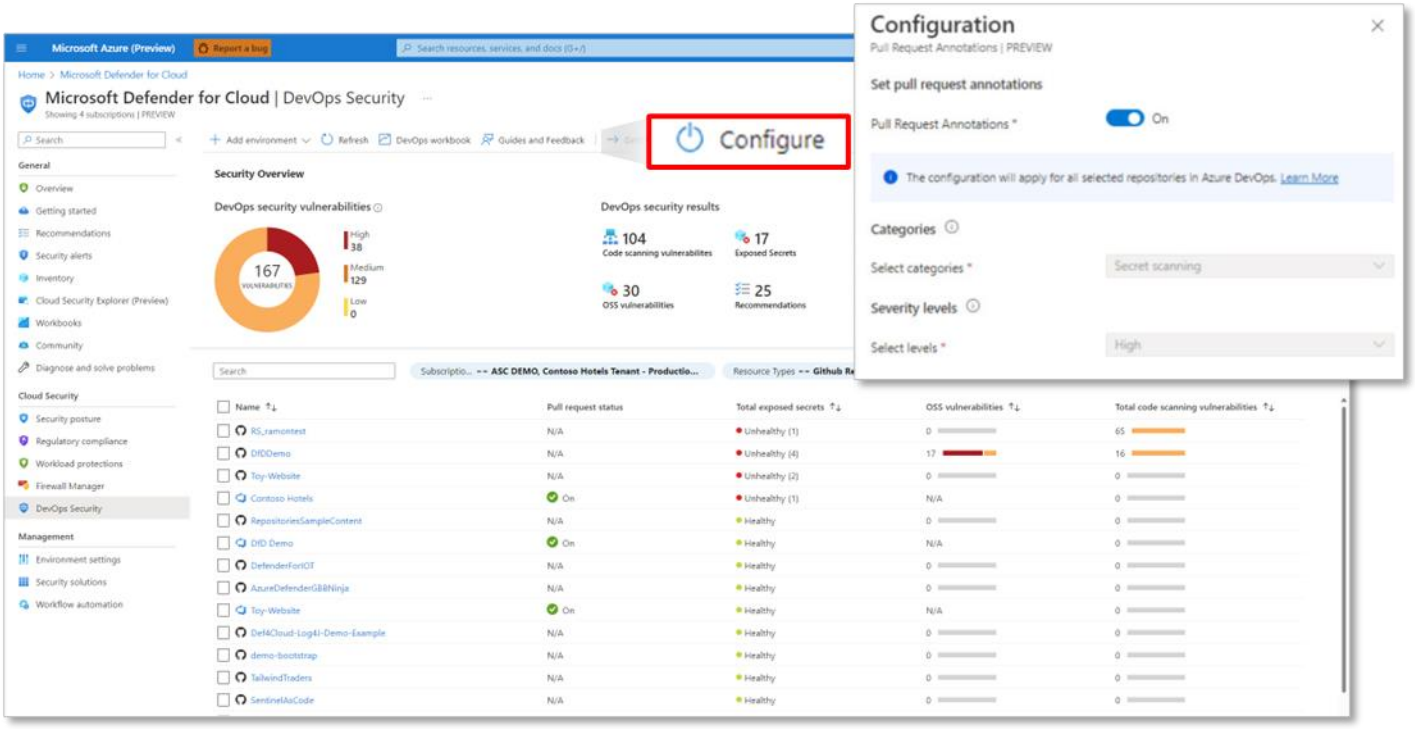


Source: ESG, a division of TechTarget, Inc.

From the DevOps security view, users would simply click *Add Connector*, then select a repository to onboard. Connectors for Azure DevOps (ADO) and Github are available. With a few clicks, ESG was able to install the Defender for DevOps app to access all repositories, and within a few minutes, the connector installation had completed and the repositories were onboarded.

Next, we clicked DevOps Security. The DevOps Security page (Figure 12) contains vulnerabilities, security results, and DevOps coverage insights into the environment to ensure that development and security teams are aligned. Next, we configured pull request annotations to enhance communication between developers and security administrators.

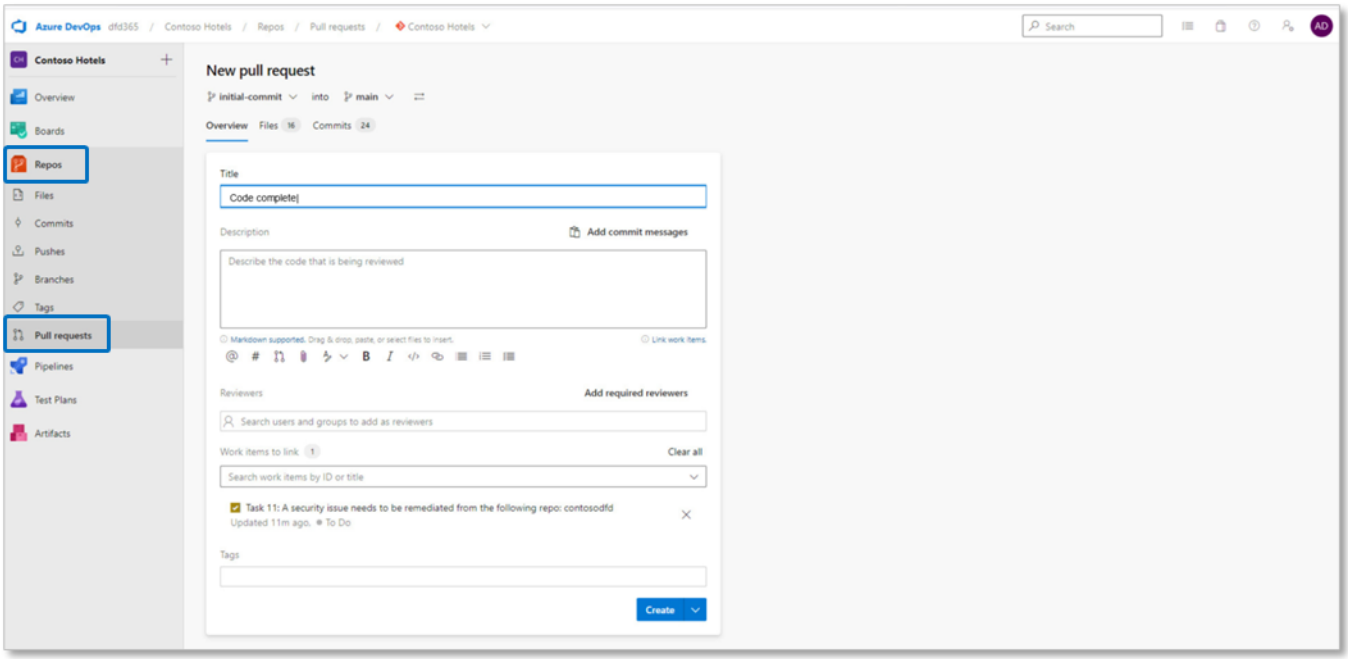
Figure 12. DevOps Security



Source: ESG, a division of TechTarget, Inc.

We selected a repository, clicked *Configure,* clicked the slider to enable pull request annotations, then clicked *Save*. Once enabled, developers can configure pull requests with a few clicks, an example using Azure DevOps as seen in Figure 12.

Figure 13. Pull Request Annotations



Source: ESG, a division of TechTarget, Inc.

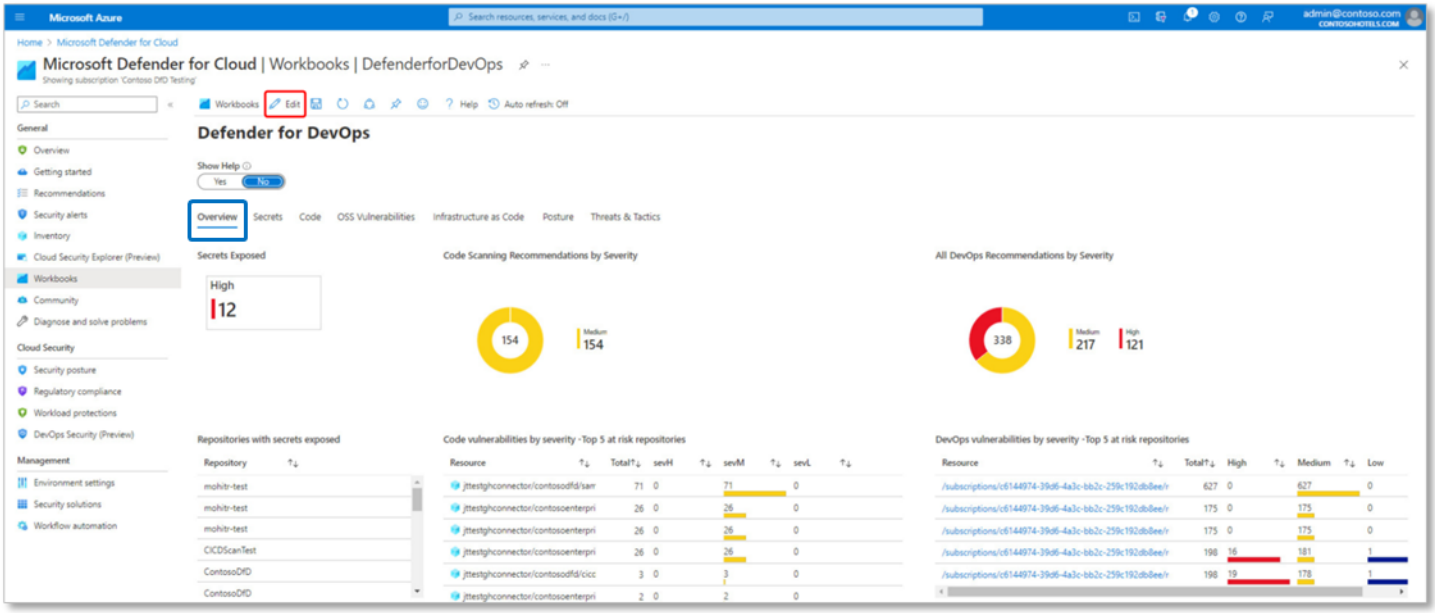
Once created, Defender for DevOps scans the pull request for vulnerabilities in the background. If a vulnerability is detected, the build will fail and the pull request annotation will inform teams of the specifics of the vulnerability, so developers can remediate the finding and resubmit the pull request.

Organizations can unify DevOps visibility using the Microsoft Security DevOps extension to expedite security tool configuration. To run the tools, all an organization needs to do is get the *MicrosoftSecurityDevOps* build from the Visual Studio marketplace and add it to their Azure DevOps pipeline and/or GitHub workflow's YAML.

Once the pipeline/workflow is set up security insights will automatically flow into Defender for Cloud providing unified visibility across DevOps environments. Defender for DevOps provides detailed recommendations under two categories; *remediate vulnerabilities* and *enable enhanced security features*. Defender for Cloud can automate the remediation process using Dependabot for GitHub repositories.

Finally, ESG looked at how organizations can obtain insights using Defender for DevOps Workbooks (Figure 14).

Figure 14. Defender for DevOps Workbooks



Source: ESG, a division of TechTarget, Inc.

This workbook pulls all information collected about repositories and scan results into a single dashboard. The *Overview* tab shows exposed secrets, code scanning vulnerabilities, and DevOps vulnerabilities. Each of the other tabs shows detailed findings, context around security posture, and threats and tactics, to help organizations target remediation and threat-hunting efforts.

Why This Matters

With the problematic shortage of cybersecurity skills, organizations need security tools that are effective and easy to use and that require little investment in training or time.

DevSecOps initiatives improve agility, can be deployed at every phase of the software lifecycle, and help enable security and compliance capabilities to be consumed as a service. By developing security as code, organizations can frontload security remediation and shift security posture management left earlier in the development cycle, so issues can be resolved sooner, wasting less effort working on flawed code and easing the burden on security administrators.

new features and capabilities can be quickly integrated into the software and applications that support data privacy and compliance programs.

ESG validated that Defender for DevOps provided comprehensive visibility into the overall security posture of a modern DevOps environment, providing deep context into the interaction and dependencies of code, entities, and infrastructure across multi-pipeline and multi-cloud environments. Most importantly, Defender for Cloud integrates this functionality seamlessly into recommendations, empowering organizations to instantly identify and remediate their most critical issues.

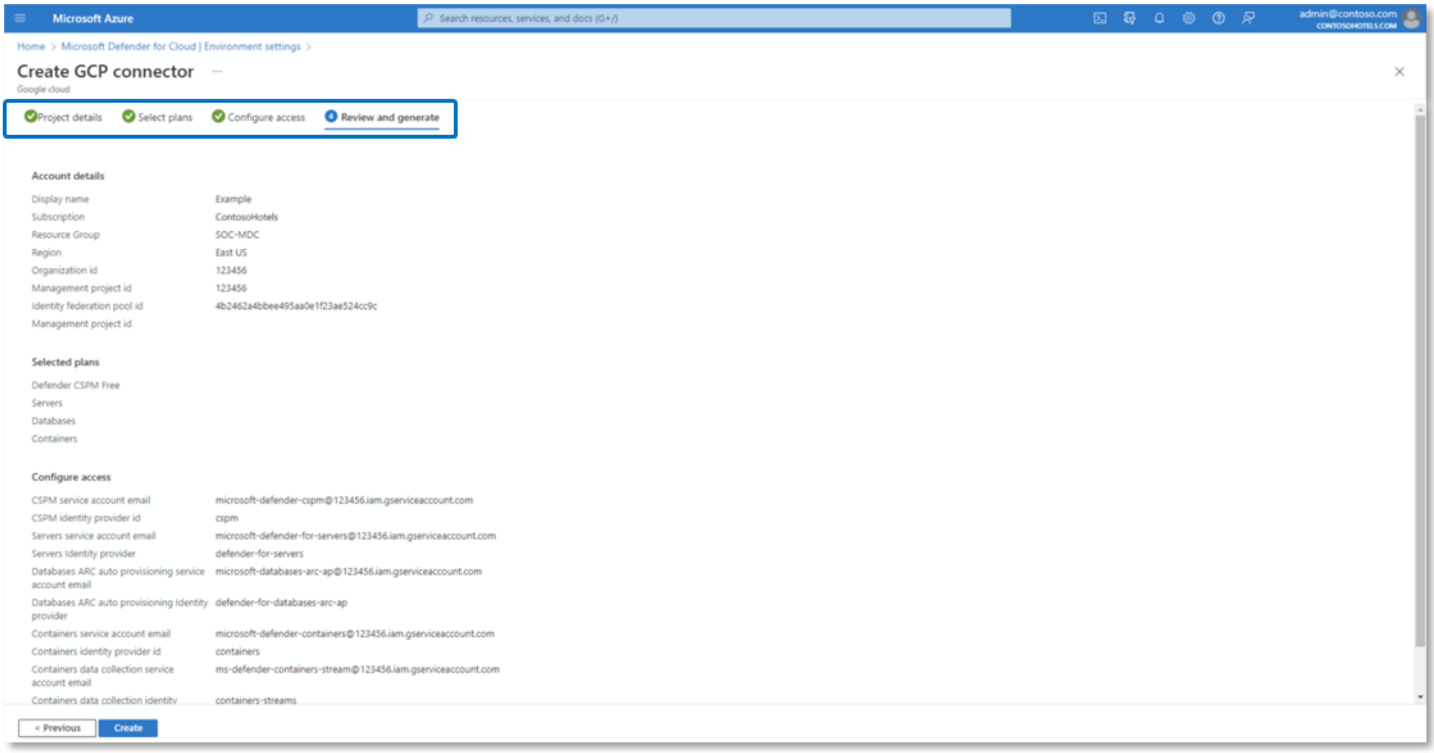
Microsoft has demonstrated a synergy between DevOps platforms—Github, Azure DevOps, and Visual Studio code—cloud platforms—Azure and multi-cloud support—and the Defender for Cloud security platform. ESG confirmed that Defender for Cloud can share visibility and improve communication between development and security teams, so security issues can be identified and resolved faster, reducing the burden on Security teams.

Detect Threats and Protect Workloads

Next, we looked at how Microsoft Defender for Cloud offers threat detection and workload protection for multiple workloads—servers, databases, storage, and containers, for example—across all layers of multi-cloud and hybrid cloud environments. ESG examined how Defender for Cloud reduces the attack surface by continuously scanning workloads to identify and manage vulnerabilities and automatically protecting new workloads when they are deployed. Defender for Cloud enables rapid response through an integrated experience with Microsoft 365 Defender and an end-to-end XDR solution.

First, ESG walked through onboarding a multi-cloud environment to protect resources across an organization. From the Defender for Cloud Overview page, we clicked on *Environment settings*, then *Add environment,* and selected Google Cloud Platform. Onboarding a new GCP project took just three steps: entering project details, selecting plans (the Defender CSPM Free plan is included for agentless discovery and continuous assessment), and configuring access (Figure 15).

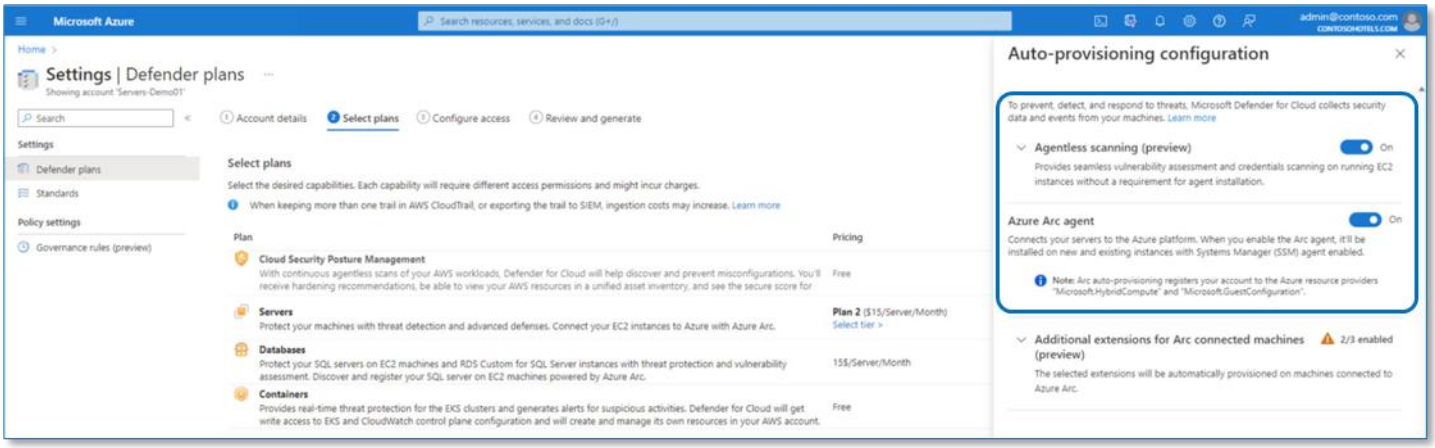
Figure 15. Onboarding a Multi-cloud Environment



Source: ESG, a division of TechTarget, Inc.

Next ESG looked at how Defender for Cloud uses agentless and agent-based scanning to provide breadth and depth of coverage of coverage across diverse clouds. We navigated to the settings page (Figure 16), then clicked Defender plans. Under *Servers*, we selected *Settings* and confirmed that agentless scanning was enabled for Amazon Elastic Compute Cloud (EC2) instances.

Figure 16. Workload Protections

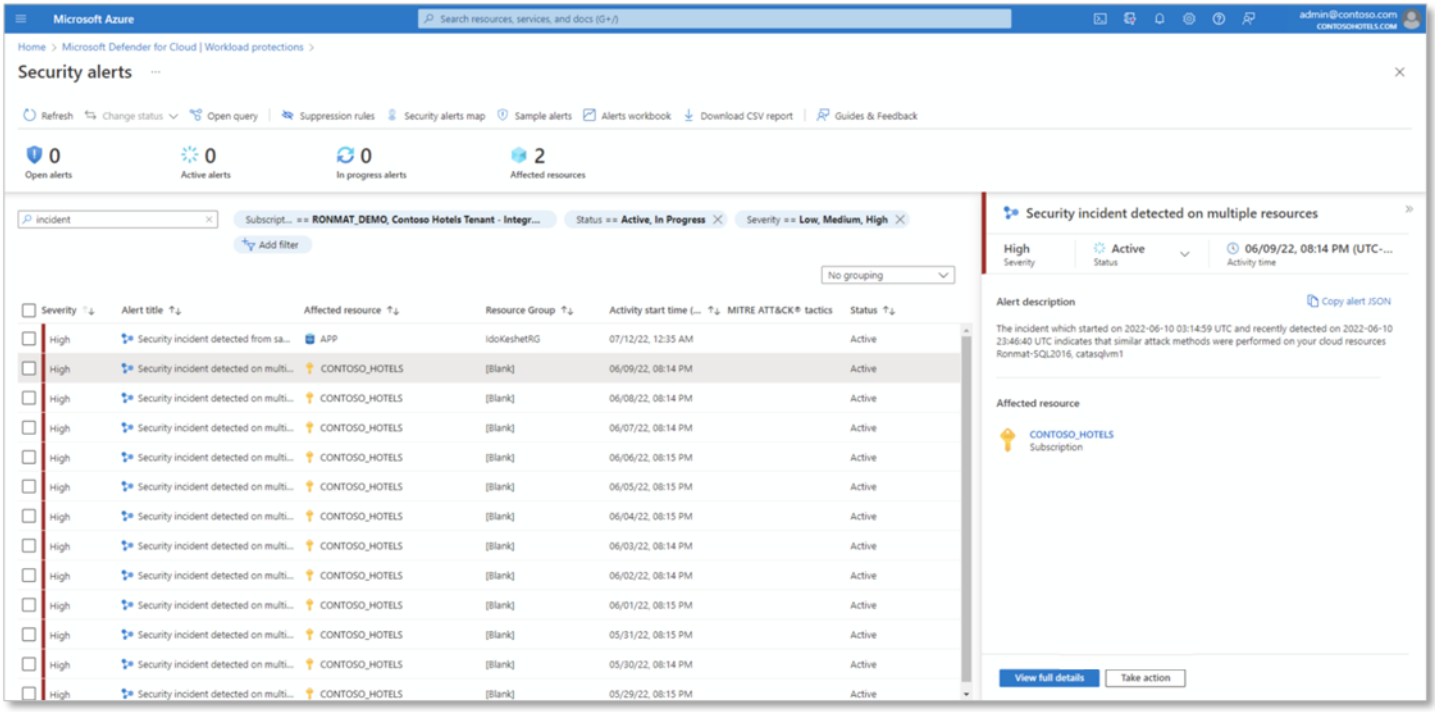


Source: ESG, a division of TechTarget, Inc.

Microsoft Defender Vulnerability management is integrated with Defender for Cloud for both agent-based and agentless scans that provide the same level of detail. Security alerts are correlated into incidents.

. ESG drilled down into an incident (Figure 17). The incident shows the affected resources and the several alerts that were correlated and combined into the security incident, enabling quick remediation with the *Take action* button.

Figure 17. Contextual Security Alert Correlation and Detections



Source: ESG, a division of TechTarget, Inc.

Microsoft Defender for Cloud protects a wide range of workload types in Azure, including servers, virtual machines, app services, containers, databases, storage, and service layer apps like DNS. Defender for Cloud also protects workload types that are native to AWS (Amazon EKS and EC2) and GCP (GKE Clusters and Google Compute).

In addition to traditional workloads like servers and containers, Microsoft Defender for Cloud also offers service layer protection for Azure. Azure Resource Manager, for example, is a critical service that is traditionally challenging to protect due to the number of logs it produces. Defender for Cloud analyzes those logs and alerts on any malicious activity to protect the top level of an organization's cloud service.

Why This Matters

The ability to prevent, detect and respond quickly to modern threats is essential to ensure security for organizations' workloads in hybrid cloud environments. How organizations respond to threats over time determines how well they can secure critical workloads across virtual machines, containers, databases, storage, and application services.

ESG validated that Defender for Cloud helps organizations focus on the most critical threats across the entire workload stack to protect workloads across hybrid cloud and multi-cloud environments from evolving threats.

ESG confirmed that the Microsoft end-to-end multi-cloud security portfolio provides unified visibility and a single control plane across multiple, diverse clouds. In addition, Microsoft combines agent-based and agentless approaches providing customers with broad and deep workload protection. This is a distinct advantage when compared to offerings that only focus on either an agentless OR agent-based approach.

The Bigger Truth

Fortified and holistic cybersecurity strategies are key to addressing the ever-expanding attack surface. Organizations are planning to increase spending on cybersecurity across multiple categories, including cloud security, data security, network security, and endpoint security, which points to the importance of taking an integrated approach to cybersecurity.

Identifying risk and ensuring that workloads are secure are basic requirements for any organization. Security policies tailored to an environment are an excellent first step. Microsoft Defender for Cloud is a centralized, integrated cloud-native protection solution that helps teams enable security across the DevOps pipeline, strengthens security posture, and protects multi-cloud workloads from complex threats.

ESG validated that Microsoft Defender for Cloud speeds time to protection, with no deployment needed in Azure and agentless onboarding for AWS and GCP. Threat prioritization and response were made easier by Defender for Cloud's ability to correlate related alerts across the entire ecosystem, from code to production, on-premises and across multiple clouds.

Defender Cloud Security Posture Management enhances visibility and identifies and reduces critical risks. Agent-based and agentless scanning quickly identifies vulnerabilities across hybrid and multi-cloud environments, while attack path analysis prioritizes the most critical risks based on potential lateral movement paths and risk context. Cloud Security Explorer's easily customizable graph-based queries enable security ops teams to identify and remediate an organization's most important threats and vulnerabilities quickly and easily.

Defender for DevOps enables organizations to secure their application workflow from code to production. Defender for DevOps detects and corrects security and quality issues as early as possible in the development cycle, preventing vulnerabilities from reaching production. Defender for DevOps facilitates communication across development, IT, and security operations teams, enabling coordinated responses to threats.

Defender for Cloud continuously scans workloads to identify and manage vulnerabilities across the entire workload stack. New workloads are automatically protected when they are deployed. Defender for Cloud enables rapid response through an integrated experience with Microsoft 365 Defender and an end-to-end XDR solution.

The results that are presented in this document are based on testing in a controlled environment. Due to the many variables in any environment, it is important to perform planning and testing in your own environment to validate the viability and efficacy of any solution.

If your organization is looking to protect workloads across its entire hybrid and multi-cloud ecosystem and is struggling with the integration of multiple, disparate tools in an attempt to strengthen its overall security posture, Microsoft Defender for Cloud is worth your serious consideration.