Technical Validation

Microsoft Defender for Cloud

Protection for Hybrid and Multi-cloud Environments

By Tony Palmer, Principal Validation Analyst
August 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 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 holistic approach to cybersecurity. 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

How will your organization’s spending in each of the following areas of cybersecurity change – if at all – over the next 12 months? (Percent of respondents, N=344)

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.
Product Page

Microsoft Defender for Cloud is a solution designed to help organizations find the weak spots across their ecosystem and strengthen their security posture while protecting their workloads in hybrid and multi-cloud environments from existing and zero-day threats. Microsoft Defender for Cloud is engineered to provide protection in the cloud across multi-cloud and on-premises assets.

Microsoft Defender for Cloud comes built into the resource provisioning process with Azure, so no 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.

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.

Figure 2. Microsoft Defender for Cloud

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 an organization from existing and zero-day advanced threats.

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.

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 3). This triggers an email alerting the resource owner that action is required.

**Figure 3. Create a Governance Rule**

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 *Owners* tab (see Figure 4) displays all owners with a summary of all recommendations that they’re assigned.

**Figure 4. Security Posture—Owner**

The *Environments* tab shows all monitored Azure subscriptions and AWS accounts with their corresponding secure score. Security Governance is scheduled for general availability on October 12th, 2022.
ESG Technical Validation

ESG examined Microsoft Defender for Cloud’s ability to provide holistic management and hardening of an organization’s security posture, its ability to detect threats and protect workloads, and how organizations could operationalize security with Defender for Cloud.

Harden and Manage Security Posture

In this section, ESG looks at Secure Score and how it helps organizations understand their security posture, implement recommendations, and monitor the state of their environment over time; how organizations can monitor and manage cloud resource inventories; and data security and compliance—identifying sensitive data and prioritizing critical resources. We then looked at how an organization would align with key compliance standards and enforce policies.

ESG Testing

First, ESG examined the security dashboard, the point of entry into the solution. The security dashboard provides a high-level overview of the security and compliance status of the whole environment across all clouds and on-premises resources (Figure 5). Secure Score is a centralized view and tracking mechanism that shows the current security state of cloud environments. The score 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.

Figure 5. The Microsoft Defender for Cloud Security Dashboard

The dashboard offers insights to help organizations quickly prioritize recommendations, identify their most-attacked resources, and act to protect them. Clicking on any widget opens a deep-dive view into that category; ESG clicked on Regulatory Compliance to drill down (Figure 6).
Security assessments are mapped to compliance controls and requirements, which enables an aggregated view of compliance status. The Azure 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. This is reflected in a higher Secure Score.

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.

### Why This Matters

Almost half (48%) of organizations report a problematic shortage of cybersecurity skills. These organizations need security tools that are effective and easy to use and that require little investment in training or time.

The Defender for Cloud Dashboard provided instant visibility into overall security posture, summaries of the several categories that make up the Secure Score with the ability to drill down. Most importantly, Defender for Cloud enables organizations to instantly identify the most relevant recommendations and the most important issues to address, with the ability to act on them with a single click. The solution enables organizations to operationalize compliance, automatically mapping recommendations to controls and requirements and providing guided resolution.

By leveraging trend analyses, organizations can see how effective their security policies and responses have been over time, pinpoint areas of potential risk, and receive guidance automatically on existing vulnerabilities they may have overlooked.
Detect Threats and Protect Workloads

Next, we look 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 the cloud and on-premises. 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 threat detection prioritizes sophisticated, resource-specific alerts based on Microsoft’s global threat intelligence across several categories, leveraging MITRE ATT&CK framework mapping to help organizations parse effects across the attack lifecycle. Alerts are correlated and grouped into incidents to speed identification, prioritization, and remediation. Vulnerabilities are exposed for fast remediation to avoid exploitation.

ESG Testing

We navigated to the workload protections dashboard (Figure 7) which presents an overview of workloads. In this view, it’s easy to identify exposed workloads and install or upgrade agents as needed. Workloads are continuously scanned to identify and manage vulnerabilities, and new workloads are automatically protected as soon as they are deployed.

Figure 7. Workload Protections

Detections are built for the unique attack vectors of each resource type, using insights gleaned from Microsoft Threat Intelligence. ESG drilled down into an incident (Figure 8). The incident shows the affected resources and the several different alerts that were correlated and combined into the security incident and enables quick remediation with the Take Action button.
Microsoft Defender for Cloud protects a wide range of workload types in Azure and those that are native to AWS (Amazon EKS and EC2) and GCP (GKE Clusters and Google Compute).

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

Why This Matters

The 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 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 Defender for Cloud identifies and prioritizes threats. It correlates alerts, combines them into incidents, and enables security professionals to focus their attention on what is most important with fast and efficient investigation and response. Service Layer protection analyzes critical cloud services to provide high-level protection.
Operationalize Security with Defender for Cloud

Finally, we reviewed how Microsoft Defender for Cloud can be operationalized to integrate hybrid and multi-cloud protection into organizations’ standard processes. In Azure, resources are automatically assessed the moment Microsoft Defender for Cloud is enabled, and workloads are protected as soon as additional protection plans are enabled. To assess AWS and GCP resources and receive security recommendations, AWS accounts/GCP projects can be onboarded with API connectors; no agents are required. For all other workloads, including those on-premises, organizations can deploy the Azure Arc agent to onboard them to Microsoft Defender for Cloud. ESG also examined how Defender for Cloud integrates with Security Information and Event Management (SIEM) systems to simplify the management of incidents.

ESG Testing

With the many tasks that a user is given as part of Secure Score, the ability to effectively remediate issues across a large fleet can feel challenging. To simplify remediation of security misconfigurations and to be able to quickly remediate recommendations on a number of resources simultaneously, Defender for Cloud offers Quick Fix remediation. This operation allows for the selection of resources to apply the remediation to and launches a remediation action that will configure the setting automatically.

Figure 9. Quick Fix Remediation—Recommendations

Organizations with centrally managed security and IT operations implement internal workflow processes to drive required actions when discrepancies are discovered in their environments. These workflows are often repeatable processes, and automation can greatly reduce overhead and streamline processes.

Organizations can create automation configurations leveraging Azure Logic Apps, then create policies to automatically trigger them based on specific findings such as Recommendations or Alerts. Azure Logic Apps can be configured to perform any custom action supported by the community of Logic App connectors or use one of the provided templates.
Organizations can export Defender for Cloud recommendations and alerts in order to enable enterprise-level scenarios. In addition to native integration with Microsoft Sentinel, recommendations and alerts can be directly exported to an Event Hub to export to a third-party SIEM, to another third-party solution in real time, or to Azure Data Explorer. Exports to Log Analytics workspaces enable the creation of custom dashboards with Microsoft Power BI.

**Why This Matters**

Assessing risk profiles and the ability to mitigate risk ensures security for organizations in the long term. How organizations respond to threats over time determines how well organizations can maintain an effective and consistent security posture.

ESG validated that organizations can use Microsoft Defender for Cloud to operationalize security by automating and integrating security into standard processes. Automatic assessment and protection in Azure, Quick Fix remediation, automation with Azure Logic Apps, and export to other Microsoft and third-party solutions enable organizations to decrease overall security risk proactively as part of their everyday operations.
**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 a holistic approach to cybersecurity.

Microsoft Defender for Cloud is designed to find the weak spots across an organization’s entire cloud configuration and help strengthen their overall security posture while protecting workloads across hybrid cloud and multi-cloud environments from evolving threats and integrating with a range of products to enable seamless response and automation for security operations teams.

Identifying risk and ensuring that workloads are secure is a basic requirement for any organization. Security policies tailored to an environment are an excellent first step. For Azure, all Defender for Cloud recommendations are built on top of Azure policy controls, enabling organizations to set policies to run on management groups, across subscriptions, or for a whole tenant.

ESG validated that Microsoft Defender for Cloud speeds time to protection with no deployment needed in Azure and agentless onboarding for AWS and GCP. We found that monitoring security posture via the dashboard was intuitive and enabled us to identify, prioritize, and respond to threats and configuration issues to harden security posture. Threat prioritization and response were made easier by Defender for Cloud’s ability to correlate related alerts into incidents. Zero-touch assessment and protection in Azure, Quick Fix bulk remediation, and automation and integration with Microsoft and third-party solutions enable comprehensive operationalization of security processes.

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 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.