# CAP Monitoring and System Activity Controls

August 8, 2022

# Revision History

| Version | Date | Description | Author |
|---|---|---|---|
| 1.0 | 08/08/2022 | Initial Draft | Brian Bolden |
| 1.1 | 10/17/2022 | Added “Associated Audits” section | Brian Bolden |
| | | | |
| | | | |
| | | | |

# Contents

# Document Details

## Stakeholders

| Stakeholder | Job Tile | Organization |
|---|---|---|
| | Senior Manager | IT Operations Services |
| | Senior Manager | App Dev & Support |
| | Technology Product Management Consultant | Digital Processing |
| Brian Bolden | Technical Writer | Digital Processing |

## Review and Approval

| Role | Name | Organization | E-Signature / Date |
|---|---|---|---|
| Reviewer | | Digital Processing | |
| Reviewer | | App Dev & Support | |
| Approver | | IT Operations Services | |

## Document Control

This document is controlled by the CAP team and is located here:

https://<location>

Any copy of this document stored or retrieved from a site other than the official site is considered uncontrolled. This procedure should be reviewed and approved annually for necessary changes.

**NOTE**: The audience for this document is internal. However, it can be provided to external users if necessary.

## Associated Audits

| Audit | Control/Requirement |
|---|---|
| HIPAA | 164.312(b): System Activity Controls |
| | 164.308(a)(1)(ii)(D): Develop and Deploy the Information System Activity Review Process |
| SOC 2 | CC4.1: CAP Software Monitoring |
| | CC4.1.6: CAP Security Operation Staffing |

## Definitions and Acronyms

| Acronym | Definition |
|---|---|
| AKS | Azure Kubernetes Service |
| AWS | Amazon Web Services |
| CAP | Company Automation Platform |

| Acronym | Definition |
|---|---|
| CSPM | Cloud Security Posture Management |
| CVE | Common Vulnerabilities and Exposures |
| CWPP | Cloud Workload Protection Platform |
| DNS | Domain Name System |
| EDR | Endpoint Detection and Response |
| GCP | Google Cloud Platform |
| IaaS | Infrastructure as a Service |
| KQL | Kusto Query Language |
| PaaS | Platform as a Service |
| SLA | Service-Level Agreement |
| SQL | Structured Query Language |
| VM | Virtual Machine |
| VMSS | Virtual Machine Scale Set |

## References

This policy references the following information sources:

| Reference/Standard/Compliance Name |
|---|
| AKS Resource Logs |
| Azure Security Benchmark |
| Cloud Monitoring Guide |
| Common and Service-Specific Schemas for Azure Resource Logs |
| Container Insights Overview |
| Microsoft Defender for Containers |
| Microsoft Defender for Kubernetes |
| Monitoring AKS Data Reference |
| Monitoring AKS with Azure Monitor |
| Regulatory Compliance Dashboard |

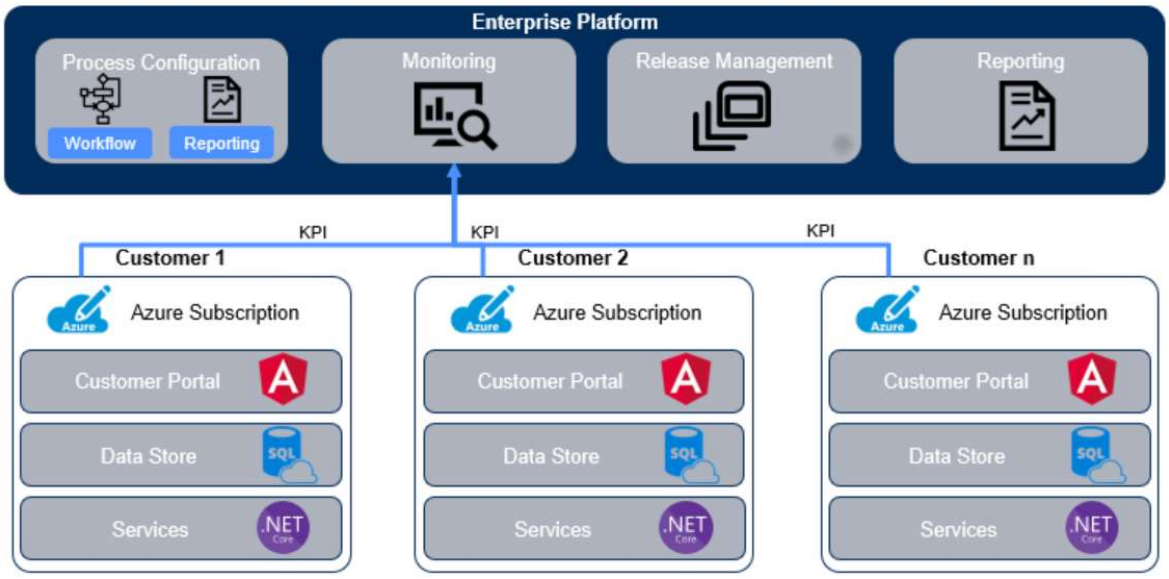
# Personnel Contact Information

| Name | Job Tile / Organization | Contact Number / E-mail |
|---|---|---|
| | Senior Manager / App Dev & Support | |
| | CAP Questions | |
| | | |
| | | |

# Introduction

## CAP Platform Overview

CAP is a cloud-based business process optimization framework running on Microsoft™ Azure cloud. It uses a micro services orchestration model to deliver extensive digital transformation portfolio via a single, unified configuration-based platform. CAP features end-to-end monitoring, reporting, security, and built-in auto-scaling with disaster recovery. The cloud-based platform architecture allows automatic updates to the latest version without taking the system out of production. The platform and its apps include built-in monitoring and alerts, providing faster resolution to client issues and reducing the frequency of those issues.




The platform consists of an Enterprise Portal and multiple Customer Portals. The Enterprise Portal is where developers create and manage business processes (blueprints, workflows, etc.) for all customers. The Customer Portal is where the customer-specific operations teams interact with the business processes used to manage their work and have access to reporting and analytics tools to keep track of SLA and work progress.

## Objective

To provide details about CAP's tools for monitoring and logging system activity, including:

- Monitoring CAP AKS with Azure Monitor
- Referencing platform metrics collected for AKS
- CAP Security Monitoring with Defender for Cloud
- Viewing logs for AKS master components and for containers in an AKS cluster
- Viewing Microsoft Defender for Kubernetes provides real-time threat protection features.

## Scope

This document provides information about the Azure and AKS monitoring and logging features that are available to CAP administrators. However, procedures for setting up these features are not included in this document. Links are provided to related Microsoft information sources that include procedures and configuration scenarios.

# CAP Monitoring

## Overview

CAP has monitoring tools in place on Microsoft Azure to evaluate system performance issues, security threats, resource utilization needs, and unusual system activity. CAP uses features of Azure Monitor to monitor the availability and performance of cloud resources on AKS. It includes a collection of telemetry critical for monitoring, analysis, and visualization of collected data to identify trends and how to configure alerting to be notified of critical issues.

The following information resources on AKS monitoring are available at https://docs.microsoft.com:

- The Cloud Monitoring Guide defines the primary monitoring objectives you should focus on for Azure resources.
- The Monitoring AKS with Azure Monitor how to use Azure Monitor to monitor the health and performance of Azure Kubernetes Service (AKS). It provides a scenario that focuses on Health and Status monitoring using Azure Monitor
- The Monitoring AKS Data Reference provides a table that lists the platform metrics collected for AKS.

While the operational data stored in Azure Monitor may be useful for investigating security incidents, other services in Azure were designed to monitor security. CAP Security Monitoring for the AKS is done with Microsoft Defender for Kubernetes.

## Features

The Azure Portal **Monitoring** menu includes features for all AKS clusters in your subscription. The screenshot below shows the **Monitoring** menu items.

**NOTE**: Can activate based on customer requests and budgeting.

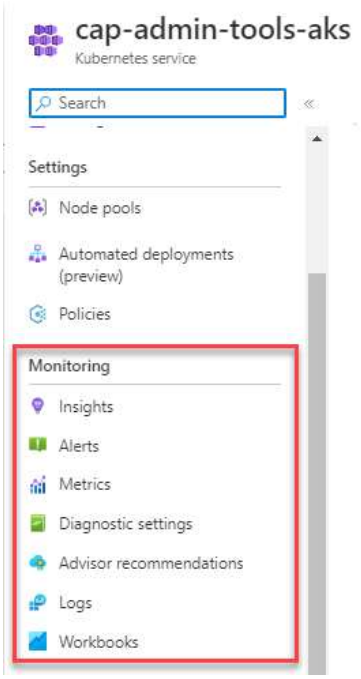



**Figure 1. Azure Portal Monitoring Menu**

| Menu Option | Descriptions |
|---|---|

| | |
|---|---|
| Insights | Opens container insights for the current cluster. Select Containers from the Monitor menu to open container insights for all clusters. |
| **NOTE**: The following Azure Monitor features are available. However, we are not using them in our CAP Enterprise deployment. | |
| Alerts | Views alerts for the current cluster. |
| Metrics | Open metrics explorer with the scope set to the current cluster. |
| Diagnostic settings | Create diagnostic settings for the cluster to collect resource logs. |
| Advisor recommendations | Recommendations for the current cluster from Azure Advisor. |
| Logs | Open Log Analytics with the scope set to the current cluster to analyze log data and access prebuilt queries. |
| Workbooks | Open workbook gallery for Kubernetes service. |

# CAP Security Monitoring

Defender for Cloud offers enhanced security features that can help protect against threats and attacks.

## Basic Security Features (Free)

By default, Defender for Cloud is enabled for free on all Azure subscriptions. It provides the secure score, security policy and basic recommendations, and network security assessment to help protect Azure resources.

## Enhanced Security Features (Paid)

Defender for Cloud enhanced security features provide unified security management and threat protection across hybrid cloud workloads. This includes:

| Feature | Description |
|---|---|
| Microsoft Defender for Endpoint | Microsoft Defender for Servers includes Microsoft Defender for Endpoint for comprehensive endpoint detection and response (EDR). Learn more about the benefits of using Microsoft Defender for Endpoint together with Defender for Cloud in Use Defender for Cloud's integrated EDR solution. |
| Vulnerability assessment for virtual machines, container registries, and SQL resources | Easily enable vulnerability assessment solutions to discover, manage, and resolve vulnerabilities. View, investigate, and remediate the findings directly from within Defender for Cloud.<br><br>**NOTE**: We currently have this activated this for SQL and Cosmos databases. |
| Multi-cloud security | Connect your accounts from Amazon Web Services (AWS) and Google Cloud Platform (GCP) to protect resources and workloads on those platforms with a range of Microsoft Defender for Cloud security features. |
| Hybrid security | Provides a unified view of security across all on-premises and cloud workloads. Allows application of security policies and continuously assess the security of your hybrid cloud workloads to ensure compliance with security standards. Collect, search, and analyze security data from multiple sources, including firewalls and other partner solutions.<br><br>**NOTE**: CAP has hybrid security capability. However, it is 100% cloud based (SaaS). |
| Threat protection alerts | Advanced behavioral analytics and the Microsoft Intelligent Security Graph provide an edge over evolving cyber-attacks. Built-in behavioral analytics and machine learning can identify attacks and zero-day exploits. Monitor networks, machines, data stores (SQL servers hosted inside and outside Azure, Azure SQL databases, Azure SQL Managed Instance, and Azure Storage) and cloud services for incoming attacks and post-breach activity. Streamline investigation with interactive tools and contextual threat intelligence.<br><br>**NOTE**: CAP does not currently use this feature. However, the capability to run it is in place. |

| Feature | Description |
| --- | --- |
| Track compliance with a range of standards | Defender for Cloud continuously assesses your hybrid cloud environment to analyze the risk factors according to the controls and best practices in Azure Security Benchmark. When you enable the enhanced security features, you can apply a range of other industry standards, regulatory standards, and benchmarks according to your organization's needs. Add standards and track your compliance with them from the regulatory compliance dashboard. |
| Access and application controls | Block malware and other unwanted applications by applying machine learning powered recommendations adapted to your specific workloads to create allow lists and blocklists. Reduce the network attack surface with just-in-time, controlled access to management ports on Azure VMs. Access and application controls drastically reduce exposure to brute force and other network attacks. |
| Container security features | Benefit from vulnerability management and real-time threat protection on your containerized environments. Charges are based on the number of unique container images pushed to your connected registry. After an image has been scanned once, you won't be charged for it again unless it's modified and pushed once more. |
| Breadth threat protection for resources connected to Azure | Cloud-native threat protection for the Azure services common to all resources:<br>• Azure Resource Manager<br>• Azure DNS<br>• Azure network layer<br>• Azure Key Vault.<br>Defender for Cloud has unique visibility into the Azure management layer and the Azure DNS layer and can therefore protect cloud resources that are connected to those layers. |

# Monitoring with Microsoft Defender for Cloud

## Overview

Microsoft Defender for Cloud is a Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) for all Azure CAP resources. Defender for Cloud fills three needs for managing resource security and workloads in the cloud and on-premises:


**Figure 2. Microsoft Defender for Cloud Resource Security Coverage**

- Defender for Cloud secure score continually assesses your security posture so you can track new security opportunities and precisely report on the progress of your security efforts.
- Defender for Cloud recommendations secures your workloads with step-by-step actions that protect your workloads from known security risks.
- Defender for Cloud alerts defends your workloads in real-time so you can react immediately and prevent security events from developing.

## IaaS and PaaS Security

In an IaaS model, you can host the workload on Azure infrastructure. Azure provides security assurances that maintain isolation and timely security updates to the infrastructure. For greater control, you host the entire IaaS solution on-premises or in a hosted data center and are responsible for security. You must implement security on the host, virtual machine, network, and storage. For example, if you have your own VNet, consider enabling Azure Private Link over Azure Monitor so you can access this over a private endpoint.

In PaaS, you have shared responsibility with Azure in protecting the data.

## Microsoft Defender Plans

CAP utilizes extended Defender for Cloud protection with advanced threat protection features. Protections include securing the management ports of your VMs with just-in-time access, and adaptive application controls to create lists for what apps should and shouldn't run on CAP machines.

The Defender plans offer comprehensive defenses for the CAP environment. These plans are listed below:

| Plan | Description |
|---|---|
| Microsoft Defender for Servers | Protects Windows and Linux machines in Azure, AWS, GCP, and on-premises. Defender for Servers provides two available plans:<br><br>**Plan 1**<br><br>• **MDE Integration**: Plan 1 integrates with Microsoft Defender for Endpoint Plan 2 to provide a full endpoint detection and response (EDR) solution for machines running a range of operating systems. Defender for Endpoint features include:<br>  ○ Reducing the attack surface for machines.<br>  ○ Providing antivirus capabilities.<br>  ○ Threat management, including threat hunting, detection, analytics, and automated investigation and response.<br>• **Provisioning**: Automatically provisions the Defender for Endpoint sensor on every supported machine that's connected to Defender for Cloud.<br>• **Licensing**: Charges Defender for Endpoint licenses per hour instead of per seat, lowering costs by protecting virtual machines only when they are in use.<br><br>**Plan 2**<br><br>• **Plan 1**: Includes everything in Defender for Servers Plan 1.<br>• **Additional features**: All other enhanced Defender for Servers security features. |
| Microsoft Defender for Storage | Detects unusual and potentially harmful attempts to access or exploit CAP storage accounts. Defender for Storage uses advanced threat detection capabilities and Microsoft Threat Intelligence data to provide contextual security alerts. These alerts include steps to mitigate the detected threats and prevent future attacks. |
| Microsoft Defender for SQL | Includes two Microsoft Defender plans that extend Microsoft Defender for Cloud's data security package to protect SQL regardless of where it is located (Azure, multi-cloud, or hybrid environments). Microsoft Defender for Azure SQL includes functions that can:<br><br>• Discover and mitigate potential database vulnerabilities.<br>• Detect anomalous activities that may be an indication of a threat to your databases. |

| Plan | Description |
| --- | --- |
| Microsoft Defender for Containers | Secures containers to improve, monitor, and maintain the security of clusters, containers, and their applications. Defender for Containers assists you with the three core aspects of container security:<br>• Environment hardening - Defender for Containers protects your Kubernetes clusters whether they're running on Azure Kubernetes Service, Kubernetes on-premises/IaaS, or Amazon EKS. Defender for Containers continuously assesses clusters to provide visibility into misconfigurations and guidelines to help mitigate identified threats.<br>• Vulnerability assessment - Vulnerability assessment and management tools for images stored in ACR registries and running in Azure Kubernetes Service.<br>• Run-time threat protection for nodes and clusters - Threat protection for clusters and Linux nodes generates security alerts for suspicious activities.<br>**NOTE**: You can learn more by watching this video from the Defender for Cloud in the Field video series: Microsoft Defender for Containers. |
| Microsoft Defender for Kubernetes (included in Microsoft Defender for Containers) | Microsoft Defender for Kubernetes provides real-time threat protection for AKS containerized environments and generates alerts for suspicious activities. You can use this information to quickly remediate security issues and improve the security of your containers. Threat protection at the cluster level is provided by the analysis of the Kubernetes audit logs.<br>**NOTE**: Microsoft Defender for Kubernetes has been replaced with Microsoft Defender for Containers. If Defender for Kubernetes is already active on a subscription, you can continue to use it. However, it will not be available for new subscriptions.<br>  <br>Figure 3. Microsoft Defender for Kubernetes Containers Activation<br>As container-specific alerts and vulnerabilities are discovered, Microsoft researchers add them to the threat intelligence feeds. Defender alerts you to any that are relevant for your environment.<br>Additionally, Microsoft Defender for Kubernetes provides cluster-level threat protection by monitoring cluster logs. This means that security alerts are only triggered for actions and deployments that occur after you've enabled Defender for Kubernetes on your subscription.<br>Examples of security events that Microsoft Defenders for Kubernetes monitors include:<br>• Exposed Kubernetes dashboards<br>• Creation of high-privileged roles<br>• Creation of sensitive mounts.<br>A full list of container alerts on Kubernetes clusters can be found here. |

| Plan | Description |
| --- | --- |
| Microsoft Defender for App Service | Identifies attacks targeting applications running over App Service. Requests to applications running in Azure go through several gateways, where they're inspected and logged. This data is then used to identify exploits and attackers and to learn new patterns that will be used later.<br><br>Azure App Service is used to build and host Web apps and APIs. It provides management, monitoring, and operational insights to meet enterprise-grade performance, security, and compliance requirements.<br><br>The following services offered by this Defender plan:<br><br>• **Secure—**Defender for App Service assesses the resources covered by the CAP App Service plan and generates security recommendations based on its findings.<br><br>• **Detect—**Defender for App Service detects threats to your App Service resources by monitoring:<br><br>  ○ The VM instance where your App Service is running and its management interface<br><br>  ○ Requests and responses sent to and from your App Service apps<br><br>  ○ Underlying sandboxes and VMs<br><br>  ○ App Service internal logs |
| Microsoft Defender for Key Vault | Safeguards encryption keys and secrets such as certificates, connection strings, and passwords. Detects unusual and potentially harmful attempts to access or exploit Key Vault accounts. This layer of protection helps to address threats without the need to manage third-party security monitoring systems.<br><br>When anomalous activities occur, Defender for Key Vault shows alerts and optionally sends them via e-mail to relevant members of your organization. These alerts include the details of the suspicious activity and recommendations on how to investigate and remediate threats. |
| Microsoft Defender for Resource Manager | Provides a management layer that enables you to create, update, and delete resources in your Azure account. CAP uses management features (access control, locks, tags, etc.) to secure and organize your resources after deployment.<br><br>Microsoft Defender for Resource Manager automatically monitors the resource management operations in your organization, whether they're performed through the Azure portal, Azure REST APIs, Azure CLI, or other Azure programmatic clients. Defender for Cloud runs advanced security analytics to detect threats and alerts you about suspicious activity. |
| Microsoft Defender for DNS | Provides an additional layer of protection for resources that use Azure DNS's Azure-provided name resolution capability. From within Azure DNS, Defender for DNS monitors the queries from these resources and detects suspicious activities without the need for any additional agents on your resources.<br><br>Microsoft Defender for DNS detects suspicious and anomalous activities such as:<br><br>• **Data exfiltration** from your Azure resources using DNS tunneling<br><br>• **Malware** communicating with command and control servers<br><br>• **DNS attacks—**communication with malicious DNS resolvers<br><br>• **Communication with domains used for malicious** activities such as phishing and crypto mining<br><br>A full list of the alerts provided by Microsoft Defender for DNS is on the alerts reference page. |

| Plan | Description |
| --- | --- |
| Microsoft Defender for open-source relational databases | Brings threat protection for the following open-source relational databases:<br>• Azure Database for PostgreSQL<br>• Azure Database for MySQL<br>• Azure Database for MariaDB<br>Defender for Cloud detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases.<br>Defender for Cloud will provide alerts when it detects anomalous database access and query patterns as well as suspicious database activities. These alerts appear in Defender for Cloud's security alerts page and include:<br>• Details of the suspicious activity that triggered them<br>• The associated MITRE ATT&CK tactic<br>• Recommended actions for how to investigate and mitigate the threat<br>• Options for continuing your investigations with Microsoft Sentinel. |
| Microsoft Defender for Azure Cosmos DB | Detects potential SQL injections based on Microsoft Threat Intelligence, suspicious access patterns, and potential exploitation of your database through compromised identities or malicious insiders.<br>Defender for Azure Cosmos DB uses advanced threat detection capabilities and Microsoft Threat Intelligence data to provide contextual security alerts. These alerts also include steps to mitigate the detected threats and prevent future attacks.<br>We have the capability to enable protection for all your databases (recommended) at either the subscription or resource level. |
| Defender Cloud Security Posture Management (CSPM) | Provides hardening guidance that helps efficiently and effectively improve your security. CSPM also gives you visibility into your current security situation.<br>Defender for Cloud continually assesses your resources, subscriptions, and organization for security issues and shows your security posture in secure score, an aggregated score of the security findings that tells you, at a glance, your current security situation: the higher the score, the lower the identified risk level.<br>The Defender CSPM plan comes with two options, foundational CSPM capabilities and Defender Cloud Security Posture Management (CSPM). When you deploy Defender for Cloud to your subscription and resources, you'll automatically gain the basic coverage offered by the CSPM plan. To gain access to the other capabilities provided by Defender CSPM, you'll need to enable the Defender Cloud Security Posture Management (CSPM) plan on your subscription and resources. |
| Defender for DevOps | Enables comprehensive visibility, posture management, and threat protection across multi-cloud environments including Azure, AWS, Google, and on-premises resources. Defender for DevOps integrates with GitHub Advanced Security that is embedded into both GitHub and Azure DevOps, to empower security teams with the ability to protect resources from code to cloud. |

# Microsoft Defender for Cloud on CAP

## Overview

Microsoft Defender for Cloud on CAP has four management dashboards:

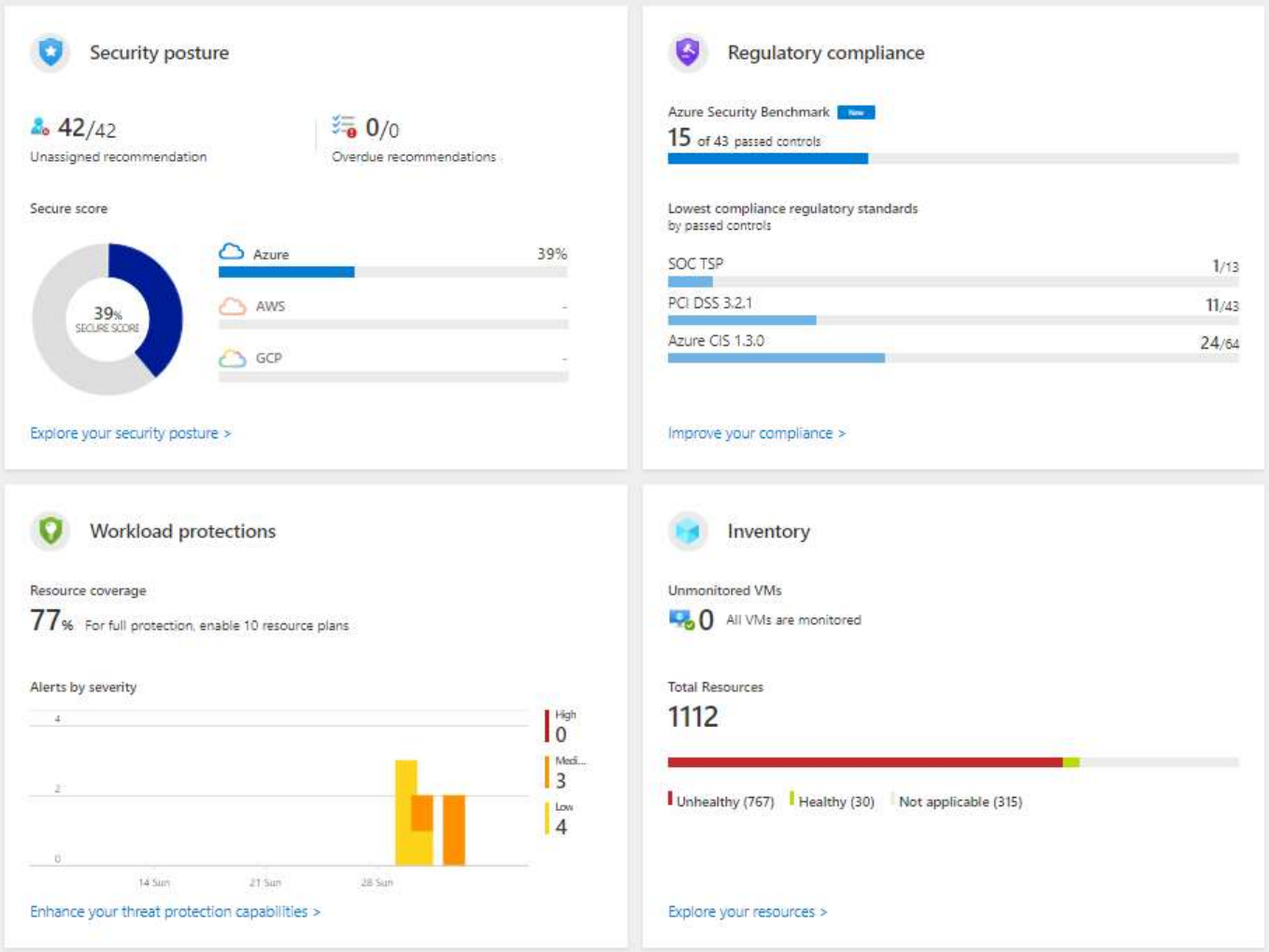



**Figure 1. Microsoft Defender for Cloud Management Dashboards**

This dashboard includes the following sections:

| Management Area | Description |
|---|---|
| Security Posture | Allows users to see the secure score for an entire subscription and for each environment in a subscription. All environments are shown by default.<br><br>**NOTE**: This feature is based on the CAP monitoring that is currently active. As CAP does not use all monitoring features, some recommendations are not warranted. |
| Regulatory Compliance | Provides insights into CAP's compliance posture based on how we are meeting specific compliance requirements. |
| Workload Protections | Provides visibility into the Microsoft Defender for Cloud coverage across different resource types. |

| Management Area | Description |
| --- | --- |
| Inventory | Provides a single page for viewing the security posture of the resources you've connected to Microsoft Defender for Cloud. All resources with unresolved security recommendations are shown in the inventory. If you've enabled the integration with Microsoft Defender for Endpoint and enabled Microsoft Defender for Servers, you'll also have access to a software inventory. The tile on the overview page provides a glance at the total healthy and unhealthy resources for the currently selected subscriptions. |

## CAP Security Posture

The Security Posture provides visibility on the CAP multi-cloud environment and includes a secure score and lifecycle management for security recommendations. The secure score measures the security posture of multi-cloud environments. The higher the score, the lower the identified risk level.

**NOTE**: As CAP is built in the Azure Cloud environment, AWS and GCP do not factor into the secure score.

On the Security posture page, users can see secure scores for each subscription and for each environment in the subscriptions. All environments are shown by default.

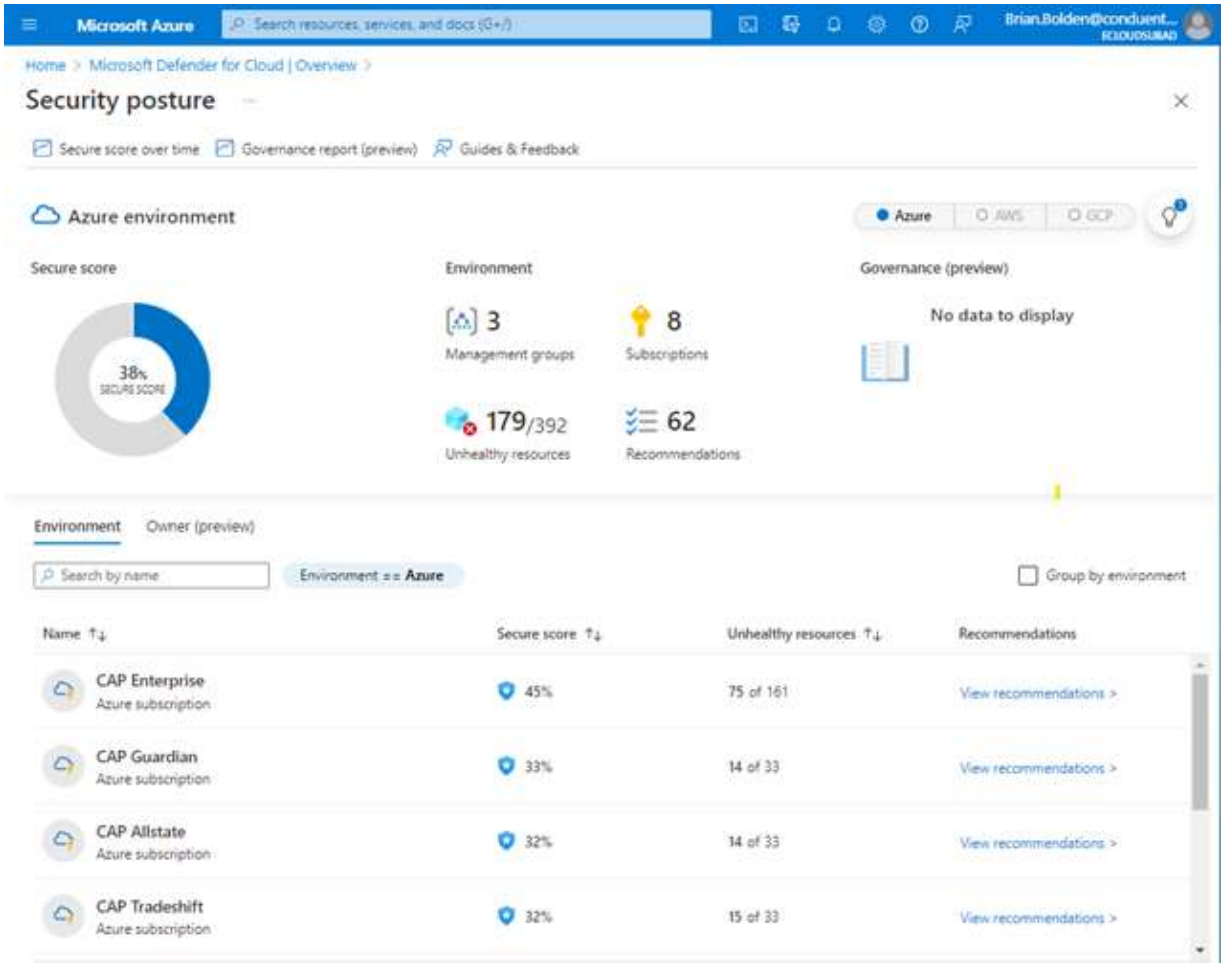



**Figure 4. Microsoft Defender for Cloud Security Posture**

The bottom section of the page includes links to Recommendations. As an example, below is a list of the **CAP Enterprise** recommendations:


**Figure 5. Microsoft Defender for Cloud Recommendations**

### Security Controls and Their Recommendations

The table below lists the security controls in Microsoft Defender for Cloud. For each control, you can see the maximum number of points you can add to your secure score if you remediate all recommendations listed in the control for all resources.

| Secure Score | Recommendation | Description |
|---|---|---|
| 10 | Enable MFA | Multi-Factor Authentication (MFA) is a security technology that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a login. Multifactor authentication combines two or more independent credentials: what the user knows, such as a password; what the user has, such as a security token; and what the user is, by using biometric verification methods.<br><br>**NOTE**: Refer to Manage multi-factor authentication (MFA) enforcement on your subscriptions and Security Control: Enable MFA for information on how to enable MFA. |
| 8 | Secure management ports | Brute force attacks often target management ports. Use these recommendations to reduce your exposure with tools like just-in-time VM access and network security groups.<br><br>**NOTE**: Refer to Security Control: Secure Management Ports for more information on this recommendation. |

| Secure Score | Recommendation | Description |
|---|---|---|
| 6 | Apply system updates | System updates bring new and enhanced features, deliver security fixes, and improve user experience to help your security posture score. Microsoft Defender for Cloud transforms system updates into several recommendations (depending on resource types) with options for addressing each one.<br><br>**NOTE**: Refer to Security recommendations—a reference guide and Security Control: Apply System Updates for information on specific system update recommendations. |
| 6 | Remediate vulnerabilities | Defender for Cloud includes multiple vulnerability assessment scanners to check your machines, databases, and container registries for weaknesses that threat actors might leverage. Use these recommendations to enable these scanners and review their findings.<br><br>**NOTE**: Refer to Security recommendations—a reference guide for more information on this recommendation. |
| 4 | Enable encryption at rest | Use these recommendations to ensure you mitigate misconfigurations around the protection of your stored data. This Security Control contains up to three recommendations (depending on the resources you have deployed in your environment). These recommendations are meant to keep your resources safe and improve your security hygiene.<br><br>**NOTE**: Refer to Security Control: Enable encryption at rest for information on how to enable this feature on Defender for Cloud. |
| 4 | Encrypt data in transit | Use these recommendations to secure data that's moving between components, locations, or programs. Such data is susceptible to man-in-the-middle attacks, eavesdropping, and session hijacking.<br><br>**NOTE**: Refer to Security Control: Encrypt data in transit for more information on this recommendation. |
| 4 | Manage access and permissions | A core part of a security program is ensuring your users have the necessary access to do their jobs but no more than that: the least privilege access model. Use these recommendations to manage your identity and access requirements.<br><br>**NOTE**: Refer to Security Control: Manage Access and Permissions for more information on this recommendation. |
| 4 | Remediate security configurations | Misconfigured IT assets have a higher risk of being attacked. Use these recommendations to harden the identified misconfigurations across your infrastructure.<br><br>**NOTE**: Refer to Security Control: Remediate Security Configurations for more information on this recommendation. |
| 4 | Restrict unauthorized network access | Azure offers a suite of tools designed to ensure access across your network meet the highest security standards.<br><br>Use these recommendations to manage Defender for Cloud's adaptive network hardening settings, ensure you've configured Azure Private Link for all relevant PaaS services, enable Azure Firewall on your virtual networks, and more.<br><br>**NOTE**: Refer to Security Control: Restrict Unauthorized Network Access for more information on this recommendation. |

| Secure Score | Recommendation | Description |
|---|---|---|
| 3 | Apply adaptive application control | Adaptive application controls are an intelligent and automated solution for defining lists of safe applications for your machines. This helps achieve multiple oversight and compliance goals by:<br>• Identifying potential malware, even any that might be missed by antimalware solutions<br>• Improving compliance with local security policies that dictate the use of only licensed software<br>• Identifying outdated or unsupported versions of applications<br>• Identifying software that's banned by your organization but is nevertheless running on your machines<br>• Increasing oversight of apps that access sensitive data.<br>**NOTES**: No enforcement options are currently available. Adaptive application controls are intended to provide security alerts if any application runs other than the ones you've defined as safe.<br>Refer to the Use adaptive application controls to reduce your machines' attack surfaces and Security Control: Apply adaptive application control for information on enabling, editing, and reviewing adaptive application controls. |
| 2 | Enable endpoint protection | Defender for Cloud checks your organization's endpoints for active threat detection and response solutions such as Microsoft Defender for Endpoint or any of the major solutions shown in this list.<br>When an Endpoint Detection and Response (EDR) solution isn't found, you can use these recommendations to deploy Microsoft Defender for Endpoint (included as part of Microsoft Defender for servers).<br>Other recommendations in this control help you deploy the Log Analytics agent and configure file integrity monitoring.<br>**NOTE**: Refer to Security Control: Enable Endpoint Protection for more information on this recommendation. |
| 1 | Enable auditing and logging | Detailed logs are a crucial part of incident investigations and many other troubleshooting operations. The recommendations in this control focus on ensuring you've enabled diagnostic logs wherever relevant.<br>**NOTE**: Refer to Set up logging to monitor logic apps in Microsoft Defender for Cloud and Security Control: Enable audit and logging for information on how to configure logging on Defender for Cloud. |

| Secure Score | Recommendation | Description |
|---|---|---|
| 0 | Enable enhanced security features | To enable all Defender for Cloud features including threat protection capabilities, you must enable enhanced security features on the subscription containing the applicable workloads.<br><br>If you only enable Defender for Cloud at the workspace level, Defender for Cloud won't enable just-in-time VM access, adaptive application controls, and network detection for Azure resources. In addition, the only Microsoft Defender plans available at the workspace level are Microsoft Defender for Servers and Microsoft Defender for SQL servers on machines.<br><br>**NOTE**: Refer to Microsoft Defender for Cloud's basic and enhanced security features and Quick start: Enable enhanced security features for more information on this recommendation. |
| 0 | Implement security best practice | This control has no impact on your secure score. For that reason, it's a collection of recommendations which are important to fulfill for the sake of your organization's security, but which we feel shouldn't be a part of how you assess your overall score.<br><br>**NOTE**: Refer to Security Control: Implement security best practices for more information on this recommendation. |

## CAP Regulatory Compliance

Microsoft Defender for Cloud compares the configuration of CAP resources with industry standard compliance requirements, regulations, and benchmarks. The regulatory compliance dashboard provides insights into your compliance posture based on how you're meeting specific compliance requirements. The CAP team has these measures in place in anticipation of customer requests.

When you've assigned a standard or benchmark to your selected scope, the standard appears in your regulatory compliance dashboard with all associated compliance data mapped as assessments. You can also download summary reports for any of the standards that have been assigned. When Microsoft releases new content for the initiative, it will appear automatically in your dashboard as new policies mapped to controls in the standard.

**NOTES:**

- To see compliance data mapped as assessments in your dashboard, add a compliance standard to your management group or subscription from within the Security policy page. To learn more about Azure Policy and initiatives, see Working with security policies.
- Refer to Customize the set of standards in your regulatory compliance dashboard for more information.

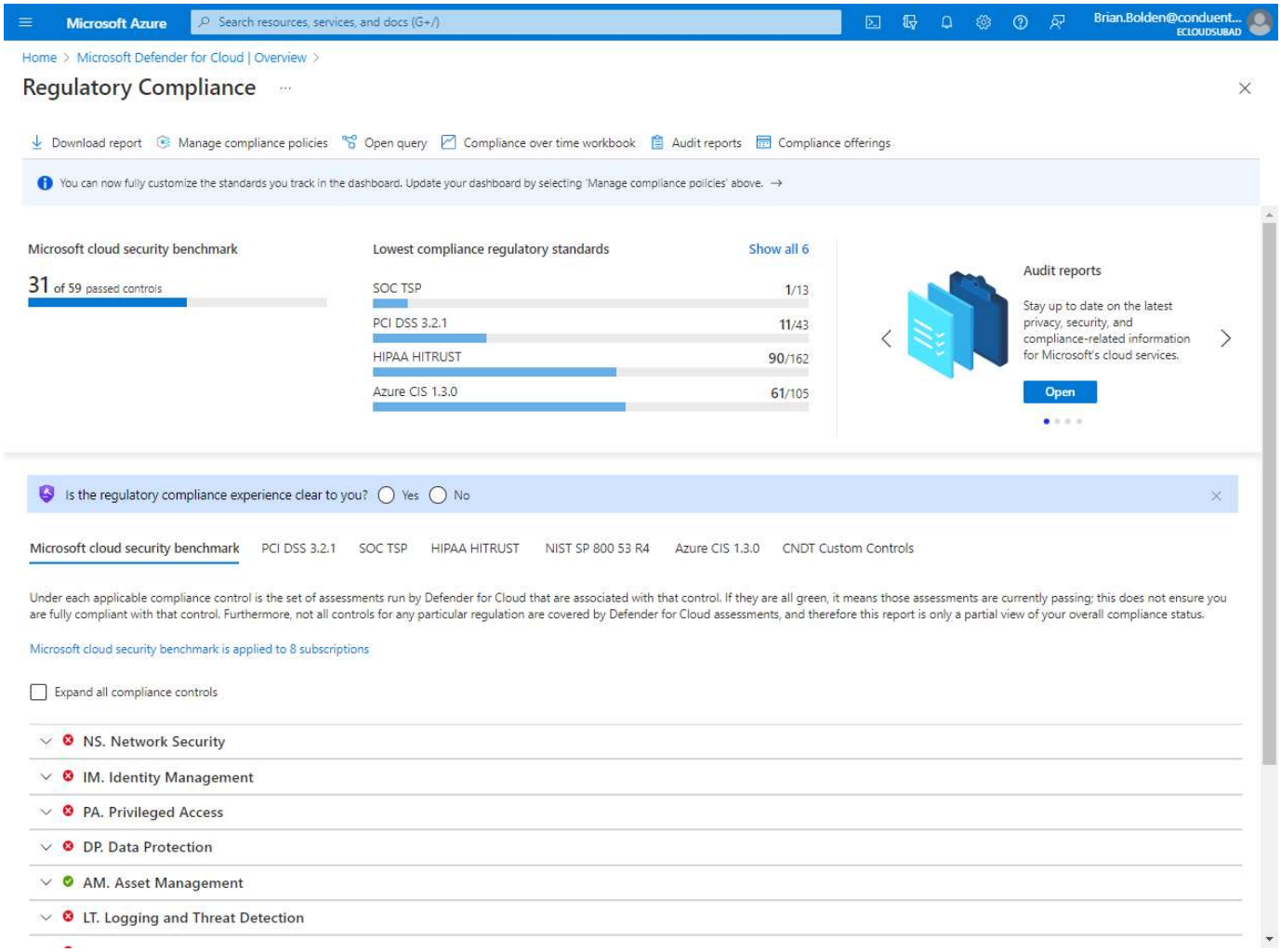



**Figure 6. Microsoft Defender for Cloud Regulatory Compliance**

## CAP Workload Protections

This dashboard provides:

- Visibility into your Microsoft Defender for Cloud coverage across your different resource types
- Links to configure advanced threat protection capabilities
- The onboarding state and agent installation
- Threat detection alerts

To access the workload protections dashboard, select Workload protections from the Cloud Security section of Defender for Cloud's menu.

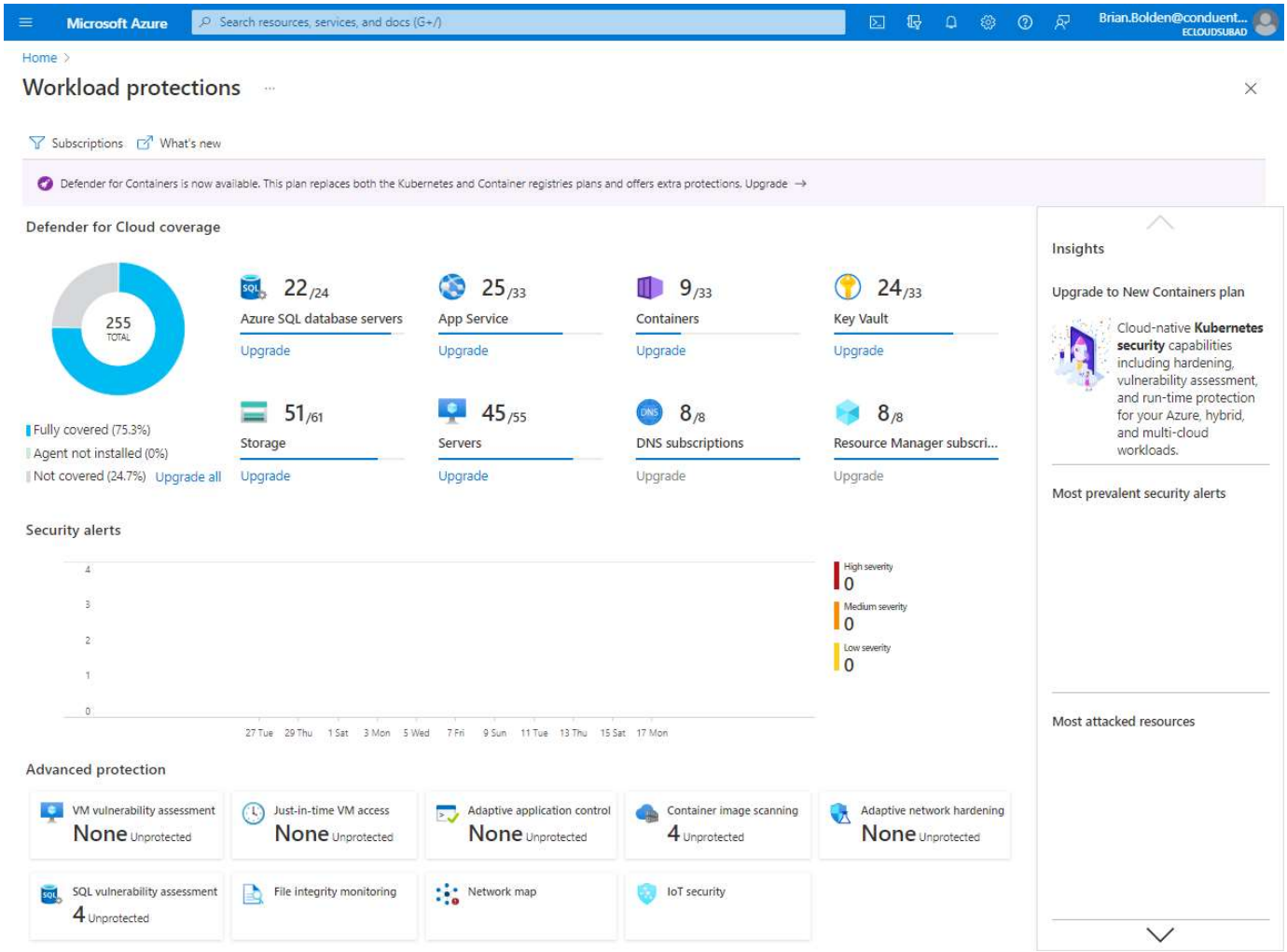



**Figure 7. Microsoft Defender for Cloud Workload Protections**

### Workload Protection Dashboard Elements

This dashboard includes the following sections:

| Section | Description |
|---|---|
| Microsoft Defender for Cloud coverage | Shows the resource types that are in your subscription and that are eligible for protection by Defender for Cloud. Wherever relevant, you'll have the option to upgrade resources. To upgrade all possible eligible resources, select **Upgrade all**.<br><br>**NOTE**: This section includes Microsoft Defender Plans for the various deployed resources. The CAP team has the capability to deploy all plans, however, not all plans are currently active. Refer to section Microsoft Defender Plans for information on the plans that appear in this section. |
| Security alerts | When Defender for Cloud detects a threat in any area of your environment, it generates an alert. These alerts describe details of the affected resources, suggested remediation steps, and in some cases an option to trigger a logic app in response. Selecting anywhere in this graph opens the Security alerts page. |
| Advanced protection | Defender for Cloud includes many advanced threat protection capabilities for virtual machines, SQL databases, containers, web applications, your network, and more. In this advanced protection section, you can see the status of the resources in your selected subscriptions for each of these protections. Select any of them to go directly to the configuration area for that protection type. |
| Insights | This rolling pane of news, suggested reading, and high priority alerts gives Defender for Cloud's insights into pressing security matters that are relevant to you and your subscription. Whether it's a list of high severity CVEs discovered on your VMs by a vulnerability analysis tool, or a new blog post by a member of the Defender for Cloud team, you'll find it here in the Insights panel. |

## CAP Asset Inventory

The asset inventory page of Microsoft Defender for Cloud provides a single page for viewing the security posture of the resources you've connected to Microsoft Defender for Cloud. Defender for Cloud periodically analyzes the security state of resources connected to your subscriptions to identify potential security vulnerabilities. It then provides you with recommendations on how to remediate those vulnerabilities. When any resource has outstanding recommendations, they'll appear in the inventory. Use this view and its filters to address such questions as:

- What subscriptions with enhanced security features enabled have outstanding recommendations?
- What machines with the tag 'Production' are missing the Log Analytics agent?
- How many of my machines tagged with a specific tag have outstanding recommendations?
- What machines in a specific resource group have a known vulnerability (using a CVE number)?

The asset management possibilities for this tool are substantial and continue to grow.

**NOTE**: The security recommendations on the asset inventory page are the same as those on the Recommendations page, but here they're shown according to the affected resource. For information about how to resolve recommendations, see [Implementing security recommendations in Microsoft Defender for Cloud].

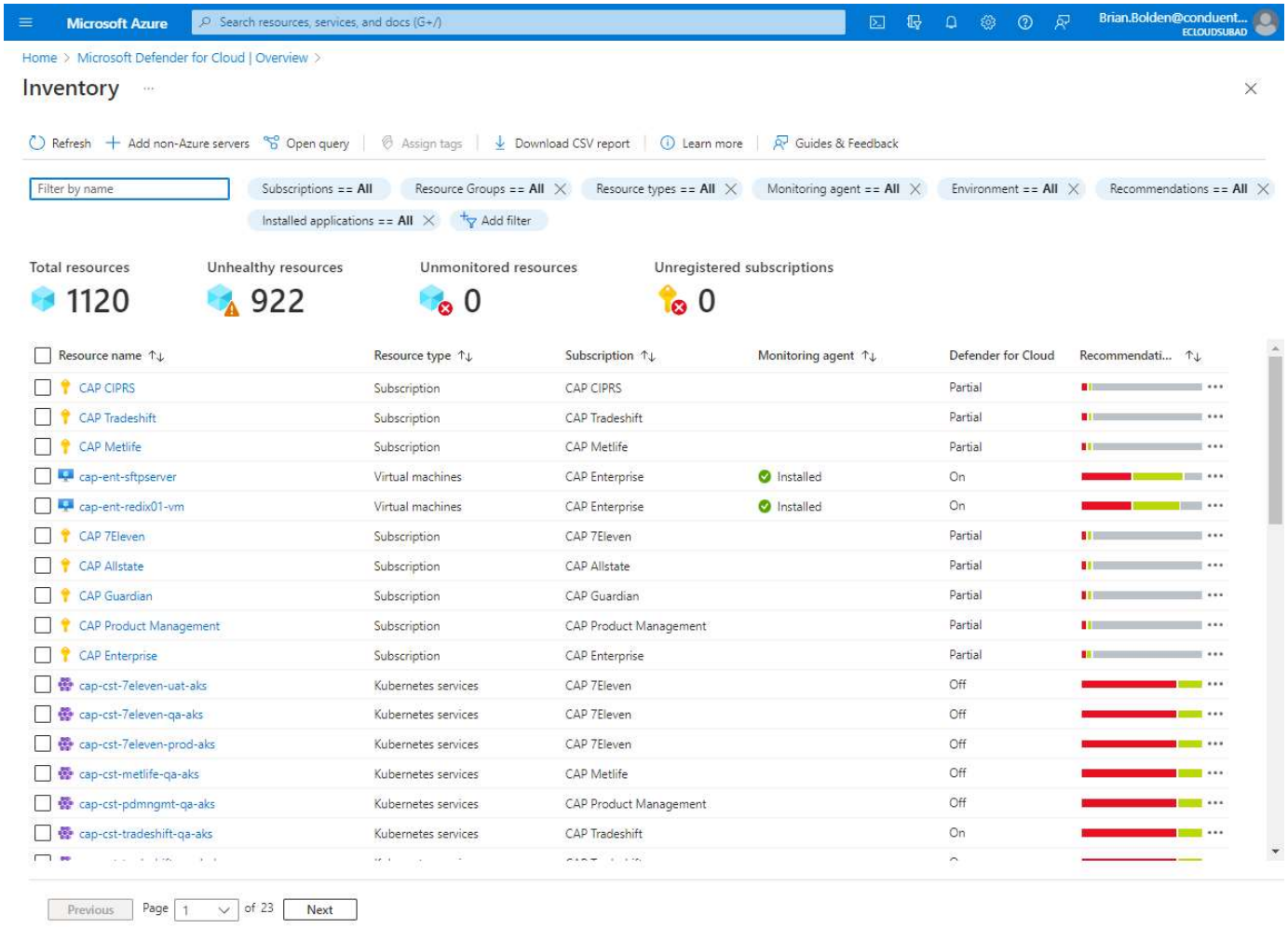



**Figure 8. Microsoft Defender for Cloud Inventory**

### Asset Inventory Dashboard Elements

This dashboard includes the following sections:

| Section | Description |
|---|---|
| Summaries | A prominent strip of values at the top of the inventory view shows:<br>• **Total resources**: The total number of resources connected to Defender for Cloud.<br>• **Unhealthy resources**: Resources with active security recommendations. Learn more about security recommendations.<br>• **Unmonitored resources**: Resources with agent monitoring issues—they have the Log Analytics agent deployed, but the agent isn't sending data or has other health issues.<br>• **Unregistered subscriptions**: Any subscription in the selected scope that haven't yet been connected to Microsoft Defender for Cloud. |
| Filters | The multiple filters at the top of the page provide a way to quickly refine the list of resources according to the question you're trying to answer. For example, if you wanted to answer the question *Which of my machines with the tag 'Production' do not have the Log Analytics agent?* by combining the **Agent monitoring** filter with the **Tags** filter.<br>As soon as you have applied the filters, the summary values are updated to relate to the query results. |
| Export and asset management tools | **Export options**: The inventory includes an option to export the results of your selected filter options to a CSV file. You can also export the query itself to Azure Resource Graph Explorer to further refine, save, or modify the Kusto Query Language (KQL) query.<br>**NOTE**: The KQL documentation provides a database with sample data and queries to see examples of the language. Learn more in this KQL tutorial.<br>**Asset management options—**When you've found the resources that match your queries, the inventory provides shortcuts for operations such as:<br>• Assign tags to the filtered resources—select the check boxes alongside the resources you want to tag.<br>• Onboard new servers to Defender for Cloud—use the **Add non-Azure servers** toolbar button.<br>• Automate workloads with Azure Logic Apps—use the **Trigger Logic App** button to run a logic app on one or more resources. Logic apps have to be prepared in advance and accept the relevant trigger type (HTTP request). Learn more about logic apps. |

**NOTE**: Refer to How does Asset Inventory work? for more information on using the Asset Inventory.

# CAP Logging

## Azure Monitor Logs

Azure Monitor Logs is an Azure Monitor feature that collects and organizes log and performance data from monitored resources. Several Azure Monitor features store their data in Logs and present this data in a variety of ways to assist in monitoring performance and availability for cloud and hybrid applications and their supporting components.

**NOTES**:

- All CAP monitoring logs go to Azure Log Analytics. While the CAP team uses Azure Log Analytics, we do not have a centralized repository for all subscription log data – we will not have the "full picture" until all log data gets sent to one workstation. Container insights data comes from log analytics.
- Azure Monitor Logs is one half of the data platform that supports Azure Monitor. The other is Azure Monitor Metrics, which stores numeric data in a time-series database. Numeric data is more lightweight than data in Azure Monitor Logs. Azure Monitor Metrics can support near real-time scenarios, so it's useful for alerting and fast detection of issues. The CAP team is not keeping track of Azure Monitor Metrics at this time.

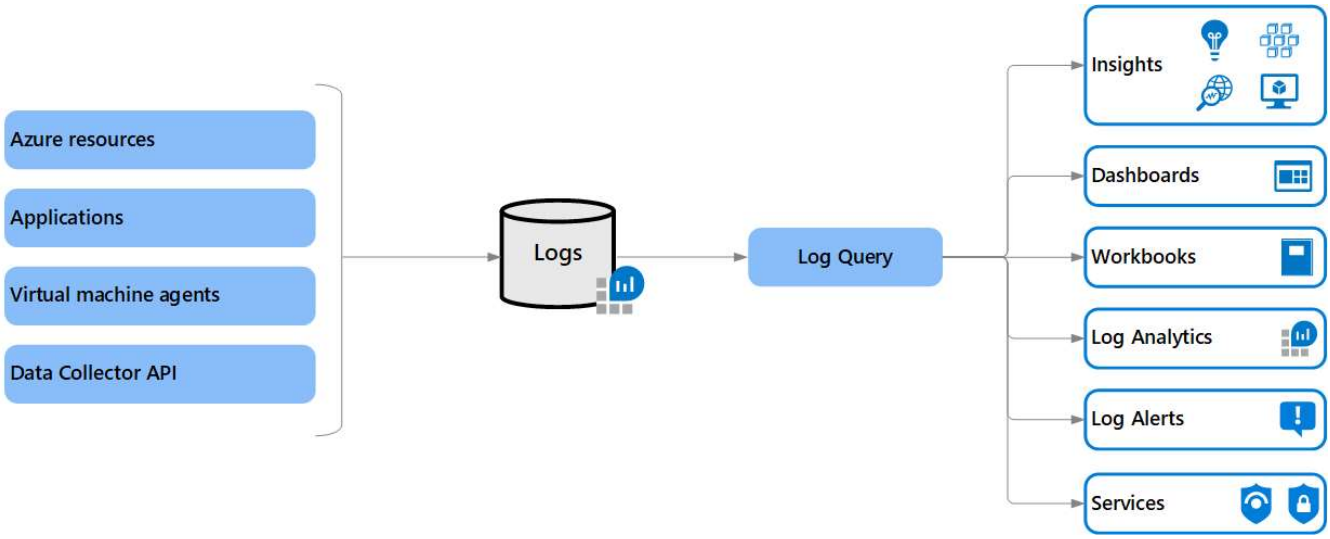



**Figure 9. CAP Logging Data Flow**

Refer to What is monitored by Azure Monitor? for a list of monitored applications and services.

## Audit Logging

Audit logging in Azure Kubernetes Service (AKS) is now generally available. Use audit logging in AKS to keep a chronological record of calls made to the Kubernetes API server (also known as the control plane), investigate suspicious API requests, collect statistics, or create monitoring alerts for unwanted API calls. Refer to Resource Logs for more information on API monitoring.

**NOTE**: There are minimal audit logging features enabled right now. Log retention is 30 days. However, it can be configured for longer.

The Resource Logs Table lists the resource log categories you can collect for AKS. These are the logs for AKS control plane components. Below are additional information sources:

- Refer to Configure monitoring for information on creating a diagnostic setting to collect resource logs and recommendations on appropriate logs to enable.
- Refer to How to query logs from Container insights for query examples on resource logs.

- Refer to Common and service-specific schemas for Azure resource logs to view logs emitted by Azure services that describe the operation of associated services and resources.

Container insights includes the Live Data feature, which is an advanced diagnostic feature allowing you direct access to your Azure Kubernetes Service (AKS) container logs (stdout/stderror), events, and pod metrics. It exposes direct access to `kubectl logs -c`, `kubectl get` events, and `kubectl top pods`. A console pane shows the logs, events, and metrics generated by the container engine to further assist in troubleshooting issues in real-time. The following links provide more information on real-time AKS logging:

- View AKS resource live logs
- View logs
- View events
- View metrics
- Using live data views

**NOTE**: Refer to How to view Kubernetes logs, events, and pod metrics in real-time for more information on Real-Time AKS logging.

# CAP Default Logging and Monitoring Configuration

## Overview

CAP manages logging and monitoring with Log Analytics workspaces. Each workspace has its own data repository and configuration that combines data from multiple services. The default configuration for new clients is included in the following workspaces:

- cap-cst-*client_name*-prod-logs
- cap-cst-*client_name*-qa-logs
- cap-cst-*client_name*-uat-logs

All available logging and monitoring features are active by default. Below is an example of the production log workspace for Allstate:

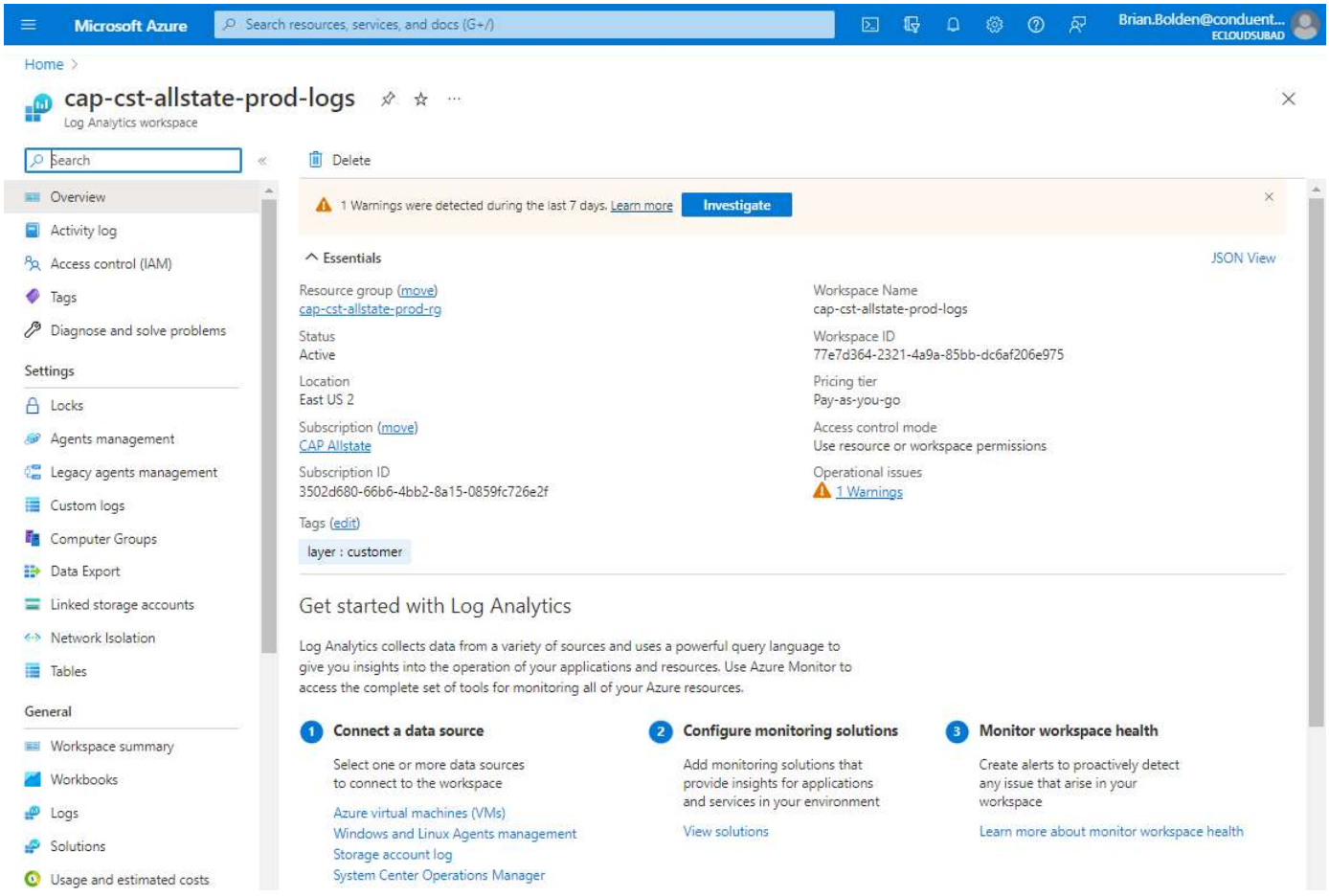



**Figure 1. Prod Log Workspace (Allstate)**

**NOTES**:

- Refer to Log Analytics workspace overview for more information on Log Analytics Workspaces.
- The CAP security administrator handles all security events and responds to alerts through Azure Defender.

# CAP Security Operation Staffing

## Overview

CAP Security Operations is staffed 24 hours a day, 7 days a week via the Global Command Center. The command center offers:

- Event monitoring through sanctioned tools on a 24x7x365 basis
- Basic triage & troubleshooting
- Service Now incident ticket creation and assignment
- Escalation to appropriate support teams
- ISP Communications

The Global Command Center resolves incidents in accordance with the Incident Management Process—SOP.