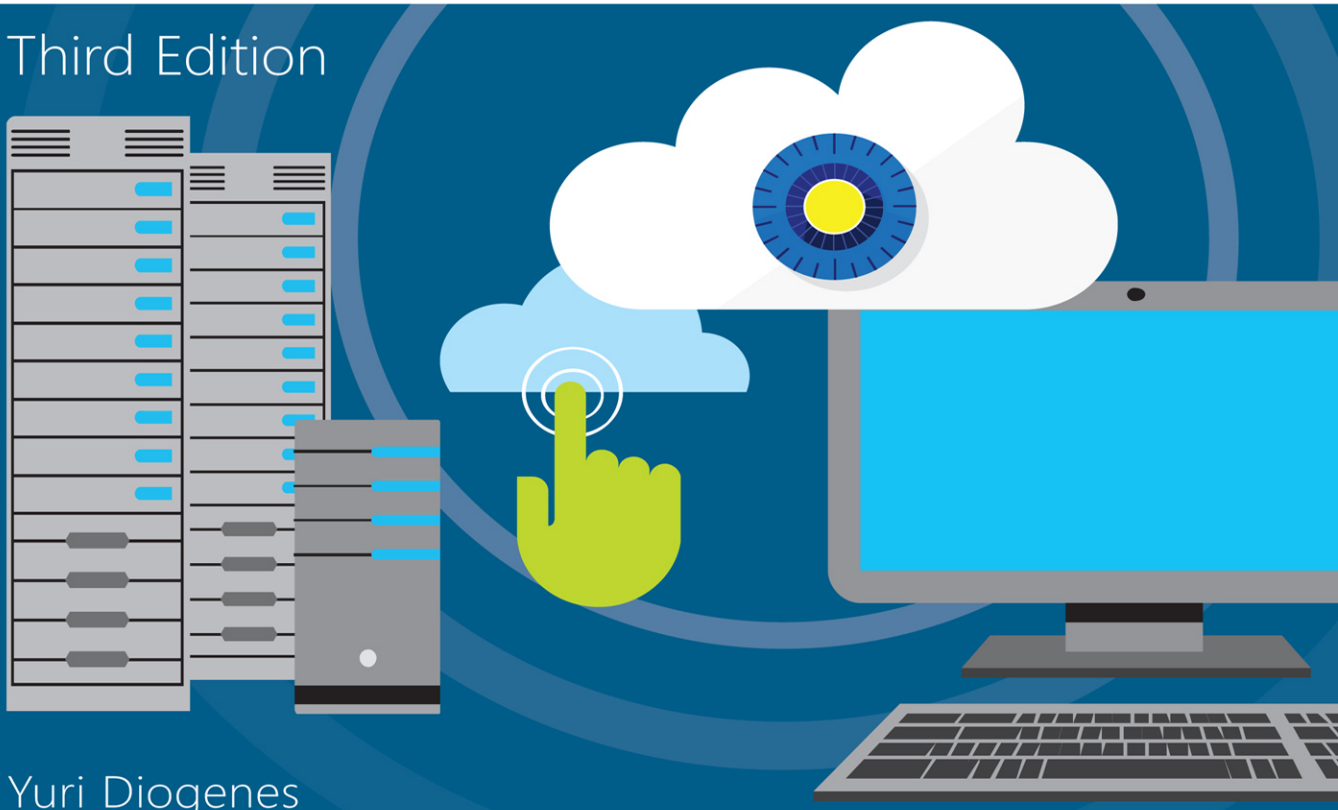
Microsoft

Microsoft Azure Security Center

Third Edition



Yuri Diogenes
Tom Janetscheck

Foreword by Bharat Shah, CVP Cloud Security at Microsoft

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Microsoft

Microsoft Azure Security Center

Third Edition

Yuri Diogenes
Tom Janetscheck

Microsoft Azure Security Center, Third Edition

Published with the authorization of Microsoft Corporation by:
Pearson Education, Inc.

ISBN-13: 978-0-13-734342-3
ISBN-10: 0-13-734342-6

Library of Congress Control Number: 2021936013

ScoutAutomatedPrintCode

EDITOR-IN-CHIEF
Brett Bartow

EXECUTIVE EDITOR
Loretta Yates

SPONSORING EDITOR
Charvi Arora

DEVELOPMENT EDITOR
Rick Kughen

MANAGING EDITOR
Sandra Schroeder

SENIOR PROJECT EDITOR
Tracey Croom

COPY EDITOR
Rick Kughen

INDEXER
Valerie Haynes Perry

PROOFREADER
Scout Festa

TECHNICAL EDITOR
Nathan Swift

COVER DESIGNER
Twist Creative, Seattle

COMPOSITOR
Danielle Foster

GRAPHICS
Vived Graphics

Contents at a Glance

	Foreword	*xv*
	Introduction	*xvii*
CHAPTER 1	**The threat landscape**	**1**
CHAPTER 2	**Introduction to Azure Security Center**	**23**
CHAPTER 3	**Policy management**	**51**
CHAPTER 4	**Strengthening your security posture**	**83**
CHAPTER 5	**Azure Defender**	**123**
CHAPTER 6	**Azure Defender for IoT**	**149**
CHAPTER 7	**Reducing the attack surface**	**161**
CHAPTER 8	**SIEM integration**	**183**
CHAPTER 9	**Accessing security alerts from API**	**195**
CHAPTER 10	**Deploying Azure Security Center at scale**	**205**
	Index	*215*

Contents

Foreword *xv*
Introduction *xvii*

Chapter 1 The threat landscape 1

Understanding cybercrime 1
Understanding the cyber kill chain 3
Common threats 5
Building a security posture 5
Adopting an assume breach mentality 7
Cloud threats and security 7
Compliance 9
Risk management 10
Identity and access management 10
Operational security 10
Endpoint protection 11
Data protection 11
Azure Security 12
VM protection 13
Network protection 14
Storage protection 17
Identity 19
Logging 20
Container security 21

Chapter 2 Introduction to Azure Security Center 23

Deployment scenarios 23
Understanding Security Center 24
Security Center architecture 25
Security Center dashboard 29

Planning adoption 30
Roles and permissions 30
Centralized management 31
Storage 31
Recommendations 32
Automation 32
Incorporating Security Center into your security operations 32
Onboarding resources 34
Auto provisioning 37
Onboard virtual machines located on-premises 39
Onboard resources from other cloud providers 43
Onboard resources using PowerShell 47
Inventory 48

Chapter 3 Policy management 51

Introduction to Azure Policy 51
Policy exemptions 54
Security Center policies 57
Fine-tuning Security Center policies 58
Creating custom policies in Azure Security Center 61
Policy enforcement and governance 64
How to overcome reactive security management 66
Prevent security misconfigurations with Security Center 66
Large-scale provisioning with Azure Blueprints 68
Policy deployment and best practices 71
Regulatory standards and compliance 73
Regulatory compliance in Azure Security Center 74
Customize your regulatory compliance experience 77
Build your own compliance initiative 78

Chapter 4 Strengthening your security posture 83

Driving security posture improvement using Secure Score 83
Fine-tuning your Secure Score 86

Create Secure Score automations with APIs and continuous export. 90
Get Secure Score data 90
Secure Score over time report 92
Secure Score decrease notification 93
Addressing recommendations 94
Enable multi-factor authentication (MFA) 95
Recommendations and controls focused on compute 99
Networking 109
Data and storage 114
Using workflow automation to remediate security recommendations . . . 118
Resource exemptions and automation 120

Chapter 5 Azure Defender 123

Introduction to Azure Defender 123
Methods of threat detection 124
Understanding alerts 124
Accessing security alerts 126
Alert suppression 129
Alerts in Azure Resource Graph (ARG) 131
Azure Defender for Servers 132
Windows 133
Linux 133
Azure Defender for Containers 134
Azure Kubernetes (AKS) 134
Azure Container Registries (ACR) 135
Azure Defender for App Service 137
Azure Defender for Storage 138
Azure Defender for SQL. 139
Vulnerability assessment for SQL 140
Azure Defender for Key Vault 143
Azure Defender for Azure Resource Manager (ARM) 144
Azure Defender for DNS 145
The cyber kill chain and fusion alerts 146

Chapter 6 Azure Defender for IoT 149

Understanding Azure Defender for IoT 149

Configuring Azure Defender for IoT 153

Security recommendations 155

Security alerts 157

Azure Defender for IoT and CyberX 158

Chapter 7 Reducing the attack surface 161

Just-in-time virtual machine access 161

Recommendation to enable JIT 163

JIT dashboard 165

Requesting access 167

File integrity monitoring 168

Customizing your settings 169

Visualizing changes 173

Adaptive Application Control 175

Configuring Adaptive Application Control 177

Chapter 8 SIEM integration 183

Streaming logs to a SIEM solution 183

Azure Sentinel 184

Integration with Azure Sentinel 186

Accessing alerts in Azure Sentinel 189

Integration with other SIEM 192

Chapter 9 Accessing security alerts from API 195

Understanding REST API 195

Accessing alerts using the Security Center REST API 196

Accessing alerts using the Graph Security API 200

Using the Graph Security API 202

Chapter 10 Deploying Azure Security Center at scale 205

The importance of management at scale 205

The three cornerstones 205

Security Center, Azure Policy, and management groups—better together 208

Best practices for managing Security Center at scale. 209

How to get started with ARM templates 210

Export templates from Azure portal 210

Use Visual Studio Code to create ARM templates 211

Index ***215***

Acknowledgments

The authors would like to thank Loretta Yates and the entire Microsoft Press/Pearson team for their support in this project, Bharat Shah for writing the foreword, and also other Microsoft colleagues that contributed by writing a sidebar for this book: Nicholas DiCola, Sarah Fender, Ram Pliskin, Laura Machado de Wright, Miri Landau, Michelle Swafford, Ajeet Prakash, John Kemnetz, Ben Nick, Phil Neray, Amit Porat, and Ariel Saghiv. We would also like to thank Nathan Swift for reviewing this book.

Yuri would also like to thank: My wife and daughters for their endless support; my great God for giving me strength and guiding my path on each step of the way; and my great friend and co-author Tom Janetscheck for this awesome partnership. I would also like to thank the Azure Security Center Engineering/Dev Teams (Gilad Elyashar, Meital Taran-Gutman, Maya Herskovic, Ron Matchoro, Tal Rosler, Ronit Reger, David Trigano, Mor Weinberger, Amit Biton, Or Serok Jeppa, Dotan Patrich, Arik Noyman, Lior Becker, Eli Sagie, Liron Kachko, Amit Magen, Miri Kreitenberger, Omer Chechik, Eli Sagie, Yossi Weizman, Hasan Abo-Shally, Shahar Weiss, Vlad Korsunsky, Jonathan Gazit, and Tamer Salman) for the ongoing collaboration and contribution. Thanks to my manager, Rebecca Halla, and my director, Nicholas DiCola, for always encouraging me to go above and beyond. Thanks to my amazing team (Safeena, Fernanda, Lior, Future, and Stan) for the continuous support and collaboration. Thanks to Devrim Iyigun for encouraging me to create the ASC in the Field Show (*aka.ms/ascinthefield*). Last but not least, thanks to my parents for working hard to give me an education, which is the foundation I use every day to keep moving forward in my career.

Tom would also like to thank: my wife and sons for always supporting me in whatever I do and for being my bastion of calm, and my great friend Yuri Diogenes for inviting me to work together on this project—it's been an awesome journey. Thanks to my manager, Rebecca Halla, my director, Nicholas DiCola, and our entire ASC CxE team: Fernanda, Future, Lior, Safeena, and Stan—you folks definitely rock, and it's my pleasure to work with all of you every day! Also, thank you to the entire Azure Security Center Engineering/Dev teams for your dedication, enthusiasm, and partnership to make ASC the great platform it is today. Last but not least, special thanks to Ben Kliger, who encouraged me to move out of my comfort zone and to take the step into Azure Security Center Engineering. This move changed my life!

About the authors

Yuri Diogenes, MsC

Yuri has a Master of Science in cybersecurity intelligence and forensics investigation (Utica College) and is the principal program manager for the Microsoft CxE ASC Team, where he primarily helps customers onboard and deploy Azure Security Center and Azure Defender as part of their security operations/incident responses. Yuri has been working in different positions for Microsoft since 2006, including five years as senior support escalation engineer in CSS Forefront Edge Team, and from 2011 to 2017 in the content development team, where he also helped create the Azure Security Center content experience since its GA launch in 2016. Yuri has published a total of 24 books, mostly about information security and Microsoft technologies. Yuri also holds an MBA and many IT/Security industry certifications such as CISSP, E|CND, E|CEH, E|CSA, E|CHFI, CompTIA Security+, CySA+, Cloud Essentials Certified, Mobility+, Network+, CASP, CyberSec First Responder, MCSE, and MCTS. You can follow Yuri on Twitter at @yuridiogenes.

Tom Janetscheck

Tom is a senior program manager for Microsoft's Azure Security Center CxE Team, where he works with his friend Yuri helping customers onboard and deploy Azure Security Center and Azure Defender. As a former Microsoft MVP, Tom joined the team during COVID-19 in Spring 2020, and he deeply misses in-person conferences because he loves to speak to audiences all over the world. With almost 20 years of experience in various IT admin and consulting roles, Tom has a deep background in IT infrastructure and security, and he holds various certifications, including MCSE and MCTS. When Tom is not writing a book, preparing a conference or user group session, or helping his customers onboard ASC, he is an enthusiastic motorcyclist and musician; he plays guitar, bass, and drums. He also volunteers as a firefighter at the local fire department and can usually be met attending rock concerts all over the place. You can follow Tom on Twitter at @azureandbeyond.

Foreword

Microsoft is just wrapping up our Solorigate investigation and have shared our final update. Cyberattacks continue to be on the rise across our customers, regardless of industry or where their resources reside, and whether it is on-premises or in the cloud. Together, we need to continue to be vigilant in protecting Azure, multi-cloud, and hybrid assets. It takes a team of both you and Microsoft to continually ensure the bad guys are kept out.

This starts with Cloud Security Posture Management (CSPM) and creating defense-in-depth for your resources. Yuri and Tom cover Azure Security Center in-depth in this book to provide you with all the insights to enable CSPM in your environments. It is imperative that you continue to strengthen your security posture using Azure Secure Score and the newly integrated Azure Security Benchmark. This is the equivalent of adding locks to your doors and windows.

While protection is a must, it is just as important to provide detection across your cloud and hybrid estate in case the thief decides to break the window! Integrated with Azure Security Center, Azure Defender provides that cloud workload protection, especially for Platform-as-a-Service (PaaS), where you are not able to do so. Yuri and Tom do a wonderful job sharing their knowledge on cyberattacks and how to respond using Azure Defender. Seconds matter, and with the knowledge they share, you can detect and respond to attacks against your workloads.

If you are an IT or Security leader, I highly recommend you share this book with your teams. It is relevant to any organization that needs to protect and defend IT workloads across clouds and hybrid environments.

Bharat Shah
Corporate Vice President
Microsoft Cloud Security

Introduction

Welcome to *Azure Security Center, Third Edition*—a book that was developed together with the Azure Security Center product group to provide in-depth information about Azure Security Center and Azure Defender, to demonstrate best practices based on real-life experience with the product in different environments.

The purpose of this book is to introduce the wide array of security features and capabilities available in Azure Security Center and Azure Defender. After being introduced to all these security options, you will dig in to see how they can be used in a number of operational security scenarios so that you can get the most out of the protection, detection, and response skills provided only by Azure Security Center and Azure Defender.

Who is this book for?

Azure Security Center is for anyone interested in Azure security: security administrators, support professionals, developers, and engineers.

Azure Security Center is designed to be useful for the entire spectrum of Azure users. You will get value from Azure Security Center regardless of whether you have no security experience, have some experience, or are a security expert. This book provides introductory, intermediate, and advanced coverage on a large swath of security issues that are addressed by Azure Security Center and Azure Defender.

The approach is a unique mix of didactic, narrative, and experiential instruction. The didactic instruction covers the core introductions to the services. The narrative instruction leverages what you already understand, and we bridge your current understanding with new concepts introduced in the book. Finally, the experience component is presented in two ways. First, we share our experiences with Azure Security Center and Azure Defender. Second, we show you how to get the most from both by providing a stepwise and guided book that helps you configure both ASC and Defender and gain all the benefits each has to offer.

In this book you will learn:

- How to secure your Azure assets, regardless of your level of security experience
- How to save hours, days, and weeks of time by eliminating the trial-and-error approach
- How to protect, detect, and respond to security threats better than ever by knowing how to get the most out of Azure Defender

System requirements

Anyone with access to a Microsoft Azure subscription can use the information in this book.

Download the code files

The sample files for this book can be downloaded from:

https://github.com/Azure/Azure-Security-Center

Errata, updates & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

MicrosoftPressStore.com/AzureSecurityCenter3E/errata

If you discover an error that is not already listed, please submit it to us at the same page.

For additional book support and information, please visit:

MicrosoftPressStore.com/Support

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *http://support.microsoft.com*.

Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

Chapter 2

Introduction to Azure Security Center

Given the threat landscape presented in Chapter 1, it is clear that there is a need for a system that can both unify security management and provide advanced threat protection for workloads running in Azure, on-premises, and on other cloud providers.

Azure Security Center gives organizations complete visibility and control over the security of hybrid cloud workloads, including compute, network, storage, identity, and application workloads. By actively monitoring these workloads, Security Center enhances the overall security posture of the cloud deployment and reduces the exposure of resources to threats. Security Center also uses intelligent threat detection to assist you in protecting your environment from rapidly evolving cyberattacks.

Security Center also assesses the security of your hybrid cloud workload and provides recommendations to mitigate threats. And it provides centralized policy management to ensure compliance with company or regulatory security requirements.

In this chapter, you will learn how you can use Security Center in your security operations, you will learn key considerations for adoption, and you'll learn how to onboard resources.

Deployment scenarios

As enterprises start their journey to the cloud, they will face many challenges trying to adapt their on-premises tools to a cloud-based model. In a cloud environment, where there are different workloads to manage, it becomes imperative to have ongoing verification, and corrective actions to ensure that the security posture of those workloads are always at the highest quality possible.

Security Center has a variety of capabilities that can be used in two categories of cloud solutions:

- **Cloud Security Posture Management (CSPM)** Enable organizations to assess their cloud infrastructure to ensure compliance with industry regulations and identify security vulnerabilities in their cloud workloads.

- **Cloud Workload Protection Platform (CWPP)** Enable organizations to assess their cloud workload risks and detect threats against their server (IaaS), containers, databases (PaaS), and storage. It also allows organizations to identity faulty configurations and remediate those with security best practices recommendations. To use the CWPP capabilities you need to upgrade to Azure Defender.

Understanding Security Center

Because Security Center is an Azure service, you must have an Azure subscription to use it—even if it's just a trial subscription.

With an Azure subscription, you can activate the free tier of Security Center. This free tier monitors compute, network, storage, and application resources in Azure. It also provides security policy, security assessment, security recommendations, and the ability to connect with other security partner solutions. Organizations that are getting started with Infrastructure as a Service (IaaS) in Azure can benefit even from this free service because it will improve their security postures.

In addition to the free tier, Security Center offers an option to upgrade to Azure Defender. This option offers a complete set of security capabilities for organizations that need more control and threat detection. Specifically, migrating your Security Center subscription from the free tier to Azure Defender enable the following features:

- Security event collection and advanced search
- Network Map
- Just-in-time VM Access
- Adaptive application controls
- Regulatory compliance reports
- File integrity monitoring
- Network Security Group (NSG) hardening
- Security alerts
- Threat protection for Azure VMs, non-Azure VMs, and PaaS services
- Integration with Microsoft Defender for Endpoint (MSDE)
- Multi-cloud support for Amazon Web Services (AWS) and Google Cloud Platform (GCP)
- Vulnerability assessment integration with Qualys

Another advantage of upgrading to Azure Defender is that it enables you to monitor on-premises resources and VMs hosted by other cloud providers. You achieve this by onboarding your machine using Azure Arc and then installing the Log Analytics agent in the target machine. (This is covered in more detail later in this chapter.)

When you upgrade to Azure Defender, you can use it free for 30 days. This is a good opportunity to evaluate these features, see how your current environment will benefit from them, and decide whether they're worth the investment. For the latest information about Azure Security Center pricing, visit *http://aka.ms/ascpricing*.

Security Center architecture

To better understand how Security Center communicates with different resources, it is important to understand its core architecture. Figure 2-1 shows the core Security Center features and how they interact with external components.

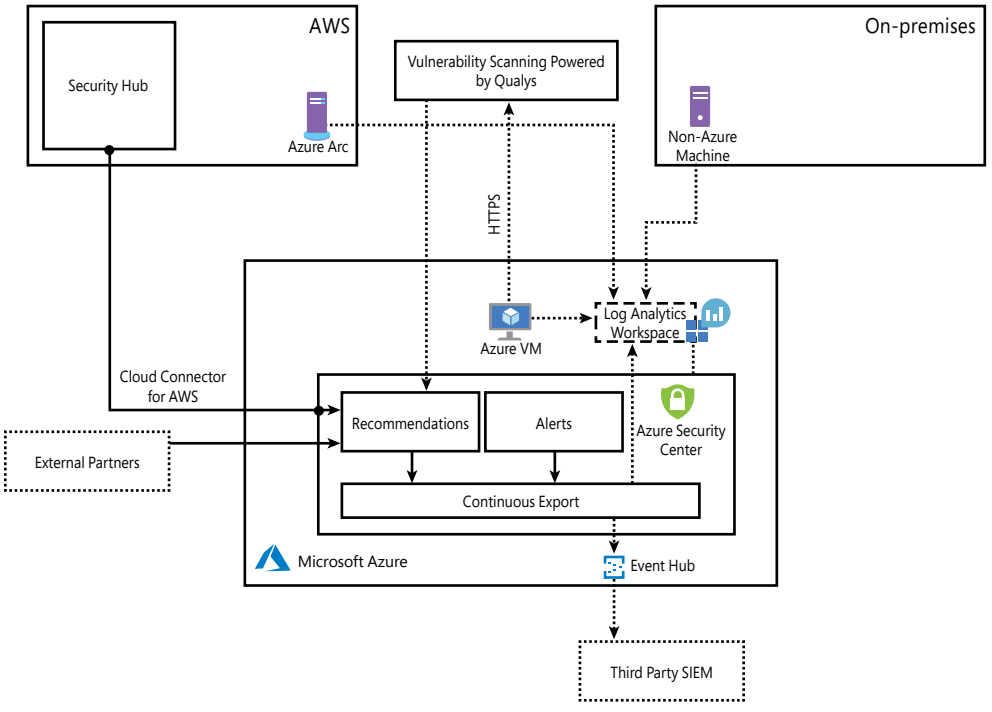


FIGURE 2-1 Connectivity between Security Center and other services

In Figure 2-1, if you look at the core diagram, which represents Security Center, you will see three major boxes: *Recommendations*, *Alerts,* and *Continuous Export*. The recommendations are an important component of the CSPM scenario because it is via the remediation of recommendations that you will enhance your security posture. *Alerts* contains the security alerts that are triggered when suspicious activities are identified. Alerts are based on a variety of threat detections, which are enabled when you upgrade to Azure Defender. Recommendations and alerts can be streamed to the Log Analytics workspace of your choice using the *Continuous Export* feature, and they can also be streamed to an Event Hub to be consumed by a third-party security information and event management (SIEM) system.

Recommendations can also be received based on the connectivity with other cloud providers such as AWS and GCP, which you will learn how to onboard later in this chapter. Another form of ingesting external recommendations is via third-party partners, which usually will be sending those recommendations via Application Program Interface (API). By the time this third edition was written, the partners available were Tenable, Cyberark, and Checkpoint.

Security Center uses the Log Analytics Agent, which is configured to send information to a particular Log Analytics workspace. Regardless of the VM location (in Azure or not), the agent must always be installed to enable Security Center to have more visibility about the machine's security events. In Windows systems, Security Center installs the Log Analytics Agent, and in Linux systems, besides the agent for Linux, Security Center also creates the `omsagent` daemon, which runs under the `omsagent` account. This account is automatically created during agent installation.

In Linux systems, Security Center collects audit records from Linux machines using the `auditd` framework (it doesn't require the `auditd` daemon to be running). The `auditd` system consists of two major components:

- First is a set of user-space utilities offering a wide collection of operations allowing administrators to better adjust rules, analyze audit log files, or troubleshoot if things are misconfigured.
- Second is a kernel-level subsystem that is responsible for monitoring system calls, filtering them by given rule set, and writing match messages to a buffer.

Both components are communicating through a `netlink` socket. `Auditd` records are collected, aggregated into events, and enriched using the latest version of the Log Analytics Agent for Linux.

In Windows systems, Log Analytics Agent scans for various security-related configurations and events in Event Tracing for Windows (ETW) traces. In addition, this agent collects the following:

- Operating system logs, such as Windows events
- Operating system type and version
- Running processes
- Machine name
- IP addresses
- Logged in user (username)
- Tenant ID
- User mode crash dump created by Windows Error Reporting (WER)

NOTE **Later in this chapter, you will learn how to change the level of granularity of the data collection for Windows systems.**

This information is sent to your workspace, which is an Azure resource used as a container to store your data. A workspace provides a geographic location for data storage, granularity for billing, and data isolation, and it helps you to better scope the configuration.

If you are using Azure Log Analytics and you already have a workspace, this workspace can be used by Security Center to store data coming from the agent. If you are not using Azure Log Analytics, a new workspace will be automatically created when you start using Security Center. The location of the workspace created by Security Center is based on the geolocation of the VM.

If you are a global company and you need to store data in specific regions for data sovereignty or compliance reasons, you might consider creating multiple workspaces. Another scenario that might call for multiple workspaces is if you want to isolate various users. For example, you might want each customer, department, or business group to see their own data but not the data for others.

> ***TIP*** **You need to use Log Analytics to create multiple workspaces. If you need to perform this operation, read this article: *https://aka.ms/ascworkspaces*.**

Once you upgrade from Security Center Free to Azure Defender, you will also have threat detection enabled for different workloads. Figure 2-2 shows how Azure Defender uses the information collected from VMs to generate a VM-based alert. In this example, non-Azure machines and Azure VMs send data collected by the agent to the workspace. Azure Defender uses this data for advanced threat detection analysis and generates recommendations that fit within the prevention module or issues alerts that are part of the detection module. Azure Defender employs advanced security analytics—a method that is far more powerful than the traditional signature-based approach.

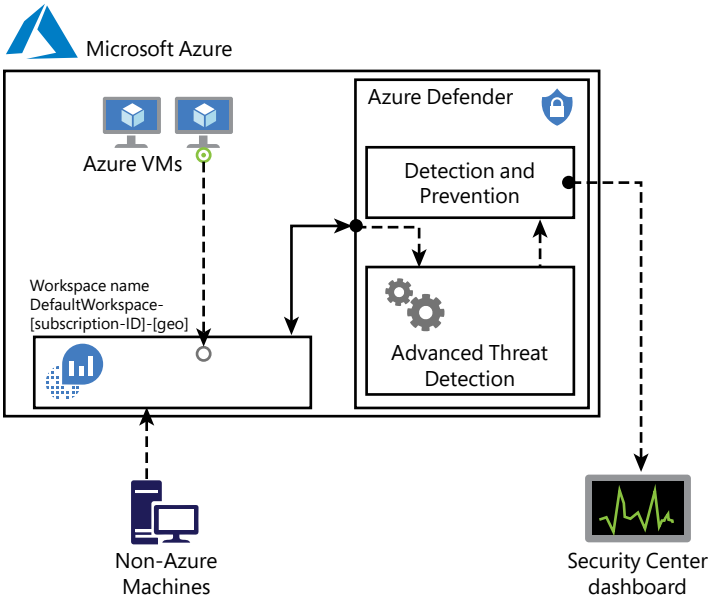


FIGURE 2-2 Azure Defender threat detection

One scenario in which multiple workspaces are needed is when you need to isolate data, such as if a company wants a separate workspace for each branch office, as shown in Figure 2-3.

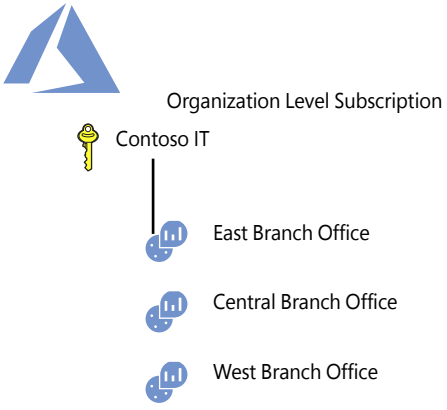


FIGURE 2-3 Workspace organization based on geolocation

Once the data is in the workspace, Azure Defender uses machine-learning technologies to evaluate all relevant events across the entire cloud fabric. By using this approach, it is possible to quickly identify threats that would be extremely hard to identify using manual processes. Azure Defender uses the following analytics:

- **Integrated threat intelligence** This leverages global threat intelligence from Microsoft to look for known bad actors.
- **Behavioral analytics** This looks for known patterns and malicious behaviors—for example, a process executed in a suspicious manner, hidden malware, an exploitation attempt, or the execution of a malicious PowerShell script.
- **Anomaly detection** This uses statistical profiling to build a historical baseline and triggers an alert based on deviations from this baseline. An example of this would be a VM that normally receives remote desktop connections 5 times a day but suddenly receives 100 connection attempts. This deviation would trigger an alert.

TIP **Read more about Azure Defender detection capabilities and other relevant scenarios at *https://aka.ms/ascdetections*.**

Security Center dashboard

To access the Security Center dashboard, sign in to Azure portal (*https://portal.azure.com*) and click **Security Center** in the left pane. What happens the first time you open the Security Center dashboard may vary. For the purposes of this example, the dashboard is fully populated with resources, recommendations, and alerts, as shown in Figure 2-4.

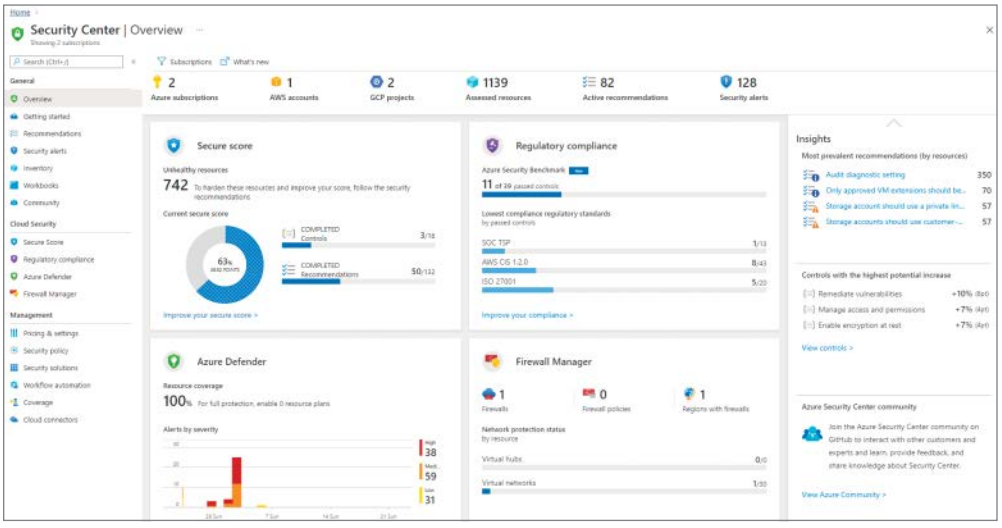


FIGURE 2-4 Security Center dashboard

As you can see in Figure 2-4, the Security Center Overview dashboard has four major areas: **Secure Score**, **Regulatory Compliance**, **Azure Defender** and **Firewall Manager**. This breakdown provides a quick overview of the main areas in Security Center. There are more options available in the left navigation pane. These options are organized in the following categories:

- **General** In this area, you will find options that can be used by your daily cloud security posture management activities, such as recommendations and inventory. It also can be used to onboard non-Azure machines and search for alerts.
- **Cloud Security** The options that are here will be used to manage your Secure Score, regulatory compliance, and to access Azure Defender features.
- **Management** The options that are here will be used to govern Security Center, including policies, workflow automation, and many others.

Throughout this book, all these options will be covered. However, for now, just browse each one of these options to familiarize yourself with the interface.

Planning adoption

Although Security Center is a cloud service, which means you don't really need to deploy any server on-premises, there are still some aspects around the adoption that you should take into consideration. One of the most critical areas is to determine who should have access to Security Center. Depending on the size and structure of your organization, multiple individuals and teams may use Security Center to perform different security-related tasks.

Roles and permissions

Security Center uses Role-Based Access Control (RBAC) based in Azure. By default, there are two roles in Security Center: Security Reader and Security Admin. The *Security Reader* role should be assigned to all users that need read access only to the dashboard. For example, security operations personnel that need to monitor and respond to security alerts should be assigned the Security Reader role. It is important to mention that the assignment of this role is done at the Azure level, under the resource group that Security Center is monitoring, and using **Access Control (IAM)**, as shown in Figure 2-5.

FIGURE 2-5 Access control in Azure

Workload owners usually need to manage a particular cloud workload and its related resources. Besides that, the workload owner is responsible for implementing and maintaining protections in accordance with company security policy. Because of those requirements, it would be appropriate to assign the *Security Admin* role to users who own a workload.

IMPORTANT **Only subscription owners/contributors and security admins can edit a security policy. Only subscription owners, resource group owners, and contributors can apply security recommendations for a resource. To enable Azure Defender, you need either the Security Admin or Subscription Owner privileges. To learn more about role-based access control (RBAC) in Azure, visit *http://aka.ms/azurerbac*.**

Centralized management

Large organizations that have different business units and are adopting Azure in a non-cohesive way might find challenges when trying to adopt Security Center because they don't have visibility of all subscriptions that are part of their tenant. For this reason, even before enabling Security Center, you need to work with your IT Team to identify all subscriptions that belong to the tenant and verify whether you have the right privileges to manage Security Center. In some scenarios, the same company might even have multiple tenants with different subscriptions on each tenant.

When multiple subscriptions are part of the same tenant and you need to centralize policy across subscriptions, you can use Azure management groups. By aggregating multiple subscriptions under the same management group, you can create one role-based access control (RBAC) assignment on the management group, which will inherit that access to all the subscriptions. This saves time on management because you can enable users to have access to everything they need instead of scripting RBAC across different subscriptions. Security Center also supports to assign security policy to a management group.

If you plan to use centralized policy management with a management group, we recommend that you remove the ASC Default initiative from the subscription since the initiative will be inherited from the management group. You can use the instructions from this article to automate this process: *http://aka.ms/ascbookmg*.

When planning your Security Center adoption, make sure to determine what needs to be monitored and whether the default policy provided by Security Center is enough for your organization or if you need to create new definitions. You will learn more about security policies in Chapter 3, "Policy management."

Storage

As explained previously, the agent will be collecting information and sending it to the workspace. If you are using Azure Defender for Server, you have up to 500 MB per day per node, and after that, Log Analytics charges will apply.

When planning Security Center adoption, consider the fact that workspaces that were created by Security Center have the data retained for 30 days. For existing workspaces, retention is based on the workspace pricing tier.

IMPORTANT **If you plan to use the same workspace for Azure Sentinel and Azure Security Center, make sure to read the best practices highlighted in this post: *http://aka.ms/ascbooklawbp*.**

Recommendations

Security Center will identify resources (compute, network, storage, identity, and application) that need security recommendations, and will automatically suggest changes. You can see all recommendations in a single place, which is available by choosing **General** > **Recommendations**. There, you have all security controls, as shown in Figure 2-6. You just need to open each security control to see the recommendations for that security control. Another option is to set the option **Group By Controls** to **Off** and see the list of all recommendations. When planning your Security Center adoption, make sure to review all recommendations before exploring more capabilities in Security Center. You should use Security Center's Secure Score impact to prioritize which security controls you should be addressing first. You will learn more about Secure Score in Chapter 4, "Strengthening your security posture."

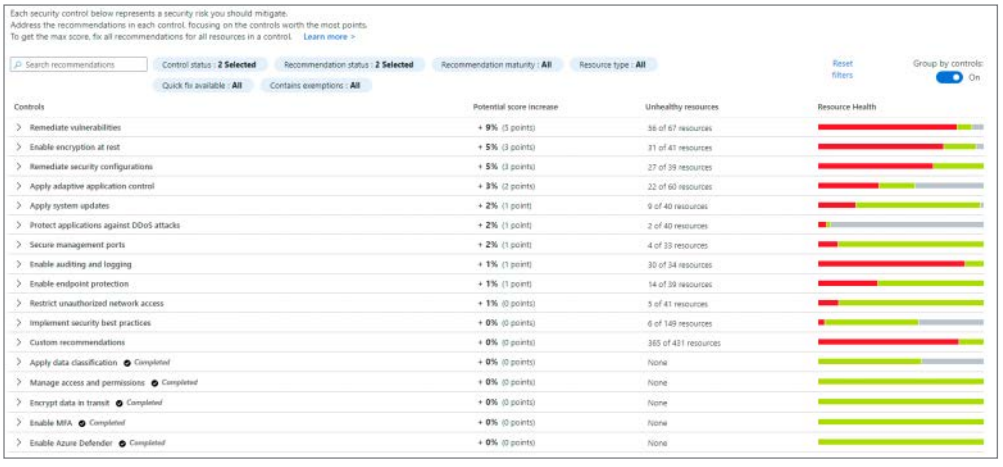


FIGURE 2-6 Aggregation of all security controls that contain recommendations in Security Center

Automation

Security Center deployment and configuration can be automated using Azure Resource Manager (ARM) templates, and PowerShell. In Chapter 10, "Deploying Azure Security Center at scale," you will learn more about the use of ARM templates for large deployments of Security Center. Later in this chapter, you will learn how to use PowerShell for task automation.

Incorporating Security Center into your security operations

It's critical that your IT security and IT operations departments constantly collaborate to provide better protection, detection, and response. Security operations (SecOps) describes this support function. Many organizations already have a SecOps team dedicated to maintaining the security operations and a cloud security posture management (CSPM) team responsible to monitor the security posture of cloud workloads. Security Center has capabilities that can be leveraged by the SecOps team, as well as by the CSPM team.

Before using Security Center to monitor resources, you must review your organization's SecOps process and identify how you can incorporate Security Center into your routine. Figure 2-7 shows the tasks performed by a typical security operations center (SOC), typical tasks for the CSPM team, and the set of Security Center features that can be leverage by these teams.

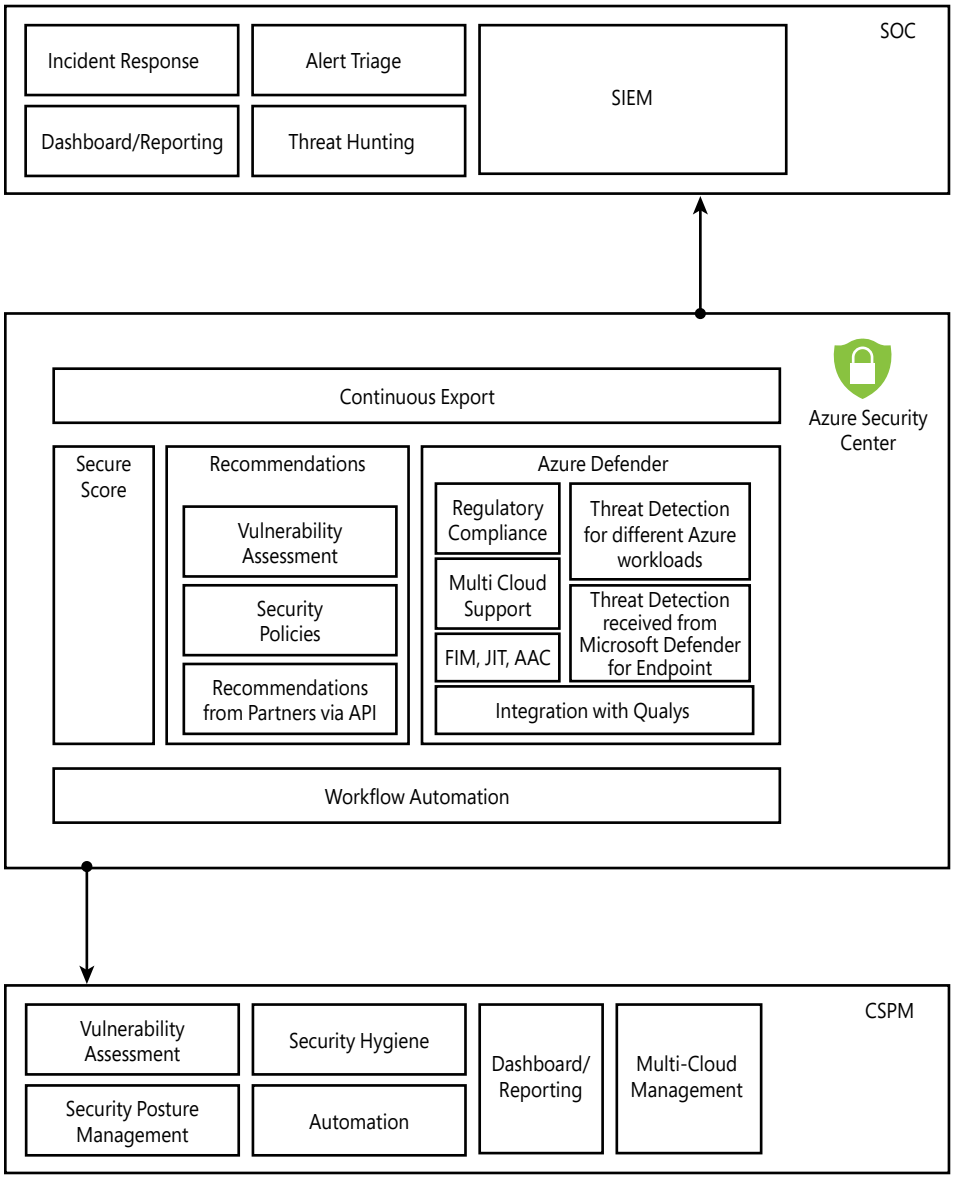


FIGURE 2-7 Mapping security operations and CSPM with Security Center

Here are a few key points for incorporating Security Center into your security operations and CSPM:

- Security Center will continuously evaluate compute, network, storage, and application resources for compliance. The CSPM team is responsible for ongoing security assessment and should track and apply recommendations issued by Security Center on an ongoing basis. This team should also leverage Secure Score as their security Key.
- Some of the capabilities that are related to CSPM, such as multi-cloud support, regulatory compliance, and Qualys integration for vulnerability assessment, will require you to upgrade your subscription to Azure Defender.
- The security roles available in Security Center, along with Azure's RBAC capability, can help SOC management control who has access to what part of the platform.
- You can leverage Azure Monitor Workbooks to provide a specific level of visualization for the SOC Team. You can leverage some workbook samples available in the Azure Security Center community page, located at *https://github.com/Azure/Azure-Security-Center/tree/master/Workbooks*.
- You should use the *Workflow Automation* feature for your CSPM team automated tasks. Make sure to leverage existing automations located on the Azure Security Center community page at *https://github.com/Azure/Azure-Security-Center/tree/master/Workflow%20automation*.
- The SOC has its own incident response (IR) team, which can consume security alerts generated by Azure Defender threat detection via the *Continuous Export* feature.
- SOC Analysts who are in charge of triaging alerts can also take advantage of Azure Defender Security Alerts dashboard to filter and suppress alerts. This team can also leverage the Workflow Automation feature to trigger response to specific alerts.

Another important consideration when incorporating Security Center as part of your SecOps is to establish how the data will be consumed by the team responsible for reviewing those alerts. Some organizations might already have a security information and event management (SIEM) system as part of their security operations, and they might not want to introduce another dashboard to their teams to query alerts. In this case, it is very common that you need to export Security Center alerts to their SIEMs by using the Continuous Export feature. In Chapter 8, "SIEM Integration," you will learn how to perform this operation.

Onboarding resources

To fully utilize all features available in Security Center, you need to first upgrade the subscription from Free to Azure Defender. You can see the current state of your subscription by clicking the **Subscription** option in the **Overview** blade. From there, you can see which subscription:

Not Covered (using free tier), **Partially Covered** (at least one workload is upgraded to use Azure Defender), or **Fully Covered** (all workloads were upgraded to Azure Defender), as shown in Figure 2-8.

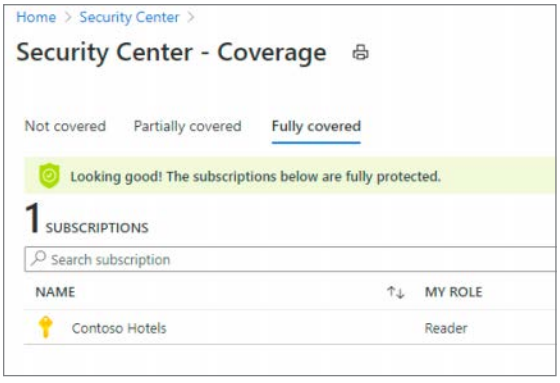


FIGURE 2-8 Subscription coverage shows the three possible states of your Azure subscription in Security Center.

If your subscription is using the Free Tier option, you can click **Getting Started** in the left navigation pane to upgrade to Azure Defender. If this is the first time you are upgrading this subscription from Free to Azure Defender, you will be able to test all capabilities for free in the first 30 days. Keep in mind that if you do not downgrade before the trial finishes, it will automatically start charging after the 30-day trial period ends. To upgrade, click the **Upgrade** button, as shown in Figure 2-9.

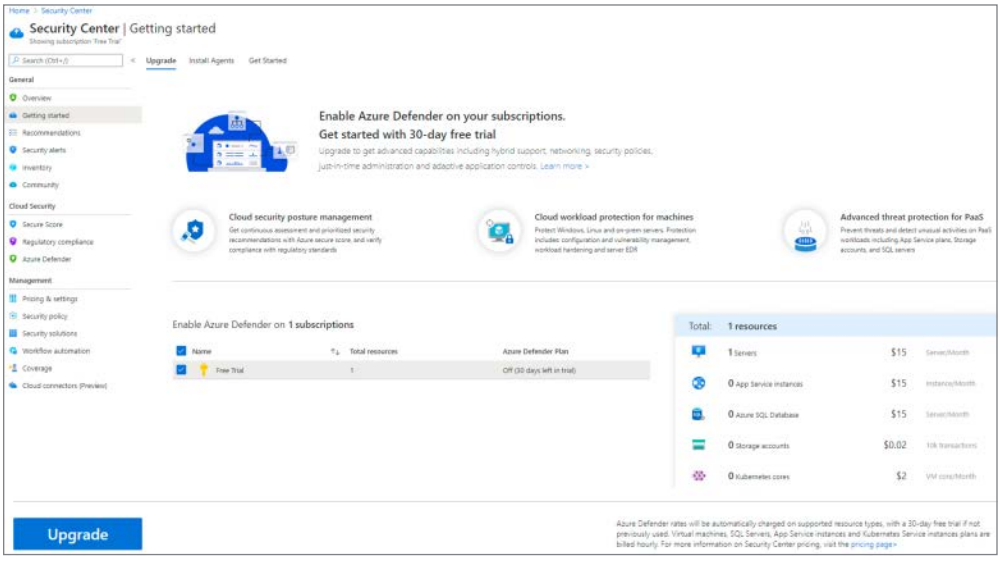


FIGURE 2-9 When you first upgrade from Free to Azure Defender, you have a 30-day free trial.

After you click this button, a notification will pop up indicating that you have started the trial, and you will be redirected to the **Install Agents** blade, as shown in Figure 2-10.

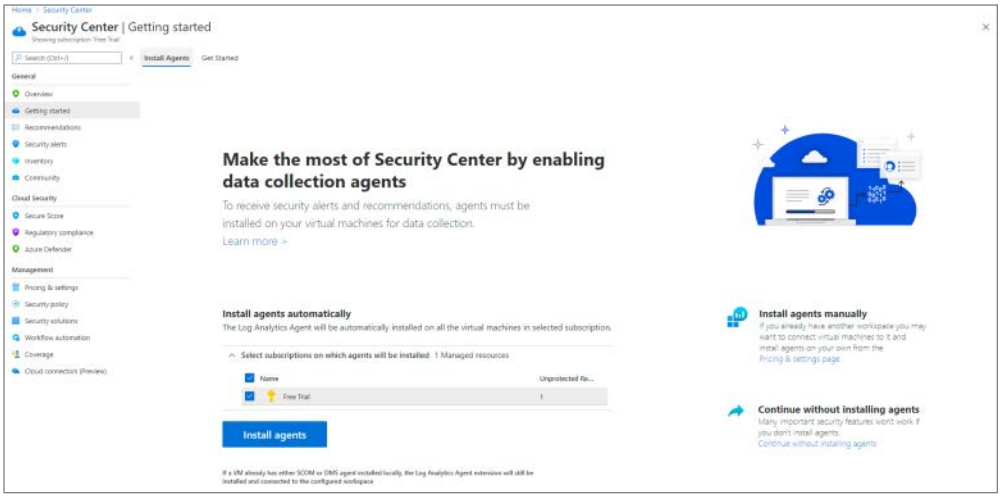


FIGURE 2-10 Options to install the agents in the selected subscriptions

To finish this step, click the **Install Agents** button, and you will be redirected back to the **Overview** page. To review pricing selection, click the **Price & Settings** option in the left navigation pane. Under **Management**, click the subscription that you just upgraded, and the **Azure Defender** plans appear, as shown in Figure 2-11.

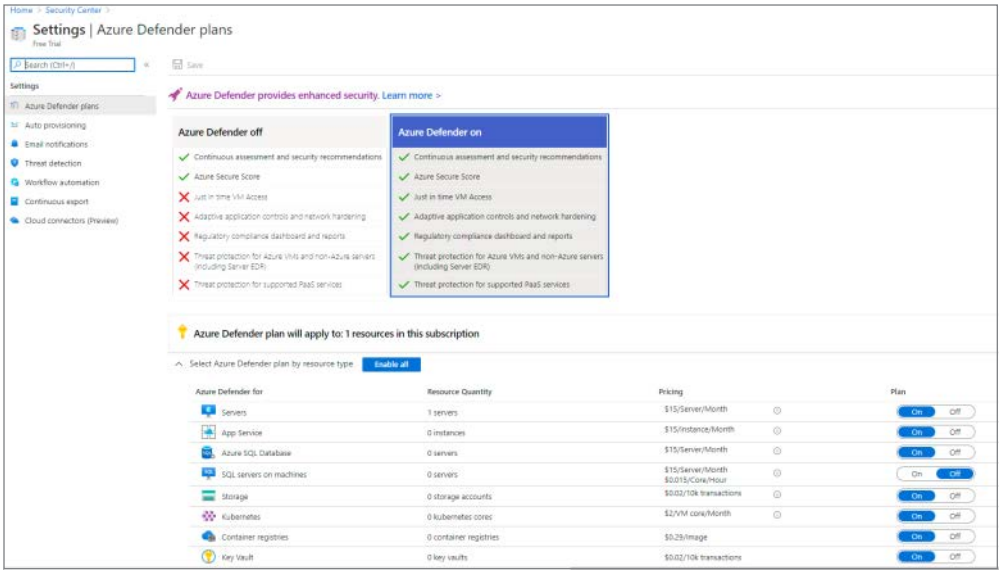


FIGURE 2-11 Azure Defender plans for different workloads

NOTE **From here on out, this book assumes you upgraded from Azure Security Free tier to Azure Defender.**

Auto provisioning

Because you selected the option to install the agents, you enabled the capability to automatically install the Log Analytics Agent on all VMs that are provisioned on this subscription. This capability is called *auto provisioning*, and it is the preferred method to configure Security Center.

However, there are some very specific scenarios in which customers may want to disable auto provisioning and control the onboarding process manually. To change these settings, follow the steps below:

1. Open the **Azure portal** and sign in as a user who has Security Admin privileges.
2. In the left navigation, click **Security Center**.
3. In the Security Center left navigation under **Management**, click the **Pricing & Settings** option.
4. Click the subscription for which you want to review the auto provisioning settings.
5. Under the **Settings** section on the left, click **Auto Provisioning**, and the Auto Provisioning settings appear, as shown in Figure 2-12.

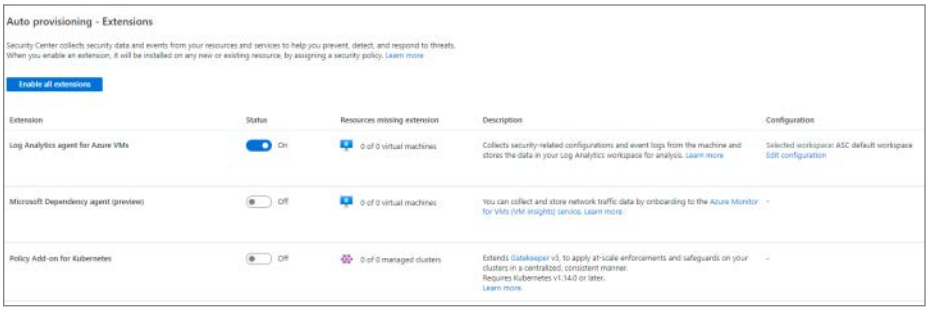


FIGURE 2-12 Auto provisioning settings in Security Center

6. In the **Configuration** column for the **Log Analytics Agent For Azure VMs**, click **Edit Configuration**.

NOTE **The steps used in this book assume that auto provisioning is enabled. If you are building a lab to simulate the steps of this book, make sure to leave auto provisioning selected.**

7. In the **Extension Deployment Configuration** blade shown in Figure 2-13, you will have the options to allow Security Center to manage the workspace (default) or select another workspace to be used by Security Center, which is the preferred option when you have multiple subscriptions and you want to centralize the workspace.

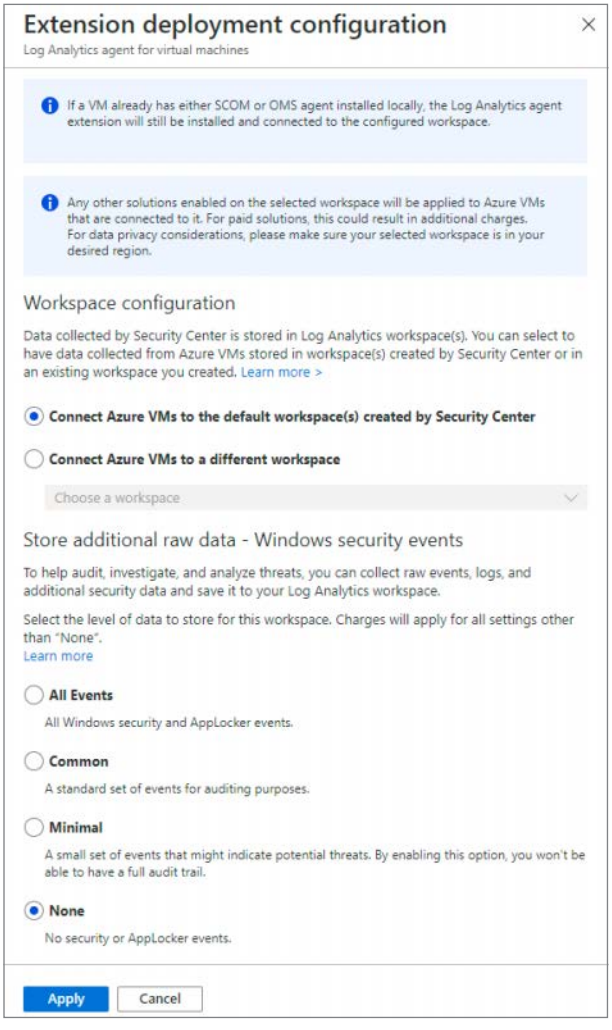


FIGURE 2-13 Options to control the workspace and data collection

NOTE **At the time this book was written, the auto provisioning feature was not available for VM Scale Set (VMSS) and Azure Kubernetes. To install the agent on those services, you need to configure an Azure Policy to deploy the agent.**

In the **Store Additional Raw Data** section, you can configure the level of data collection granularity for Windows systems. Each setting will determine the type of events that will be collected. If you are using Group Policy Object (GPO) to configure your servers where the agent will be installed, we recommend that you enable the audit policies `Process Creation Event 4688` and the `CommandLine` fields inside event `4688`. Audit Process Creation determines whether the operating system generates audit events when a process is created (starts). This information includes the name of the program or the user who created the process. Below you have a summary of what each option collects:

- **All Events** If you select this option, all security events will be stored in your workspace.
- **Common** When you select this option, only a subset of events will be stored in your workspace. Microsoft considers these events—including login and logout events—to provide sufficient detail to represent a reasonable audit trail. Other events, such as Kerberos operations, security group changes, and more, are included based on industry consensus as to what constitutes a full audit trail.
- **Minimal** Choosing this setting results in the storage of fewer events than the **Common** setting, although we aren't sure how many fewer or what types of events are omitted. Microsoft worked with customers to ensure that this configuration surfaces enough events that successful breaches are detected and that important low-volume events are recorded, but logout events aren't recorded, so it doesn't support a full user audit trail.
- **None** This option disables security event storage.

To enable data collection for Adaptive Application Controls, Security Center configures a local AppLocker policy in Audit mode to allow all applications. This will cause AppLocker to generate events that are then collected and stored in your workspace. It is important to note that this policy will not be configured on any machines on which there is already a configured AppLocker policy. To collect Windows Filtering Platform Event ID 5156, you need to enable Audit Filtering Platform Connection (`Auditpol /set /subcategory:"Filtering Platform Connection" /Success:Enable`).

NOTE **For details about the event ID that is collected for Windows, visit *http://aka.ms/ascdatacollection*.**

Onboard virtual machines located on-premises

As explained previously, VMs that are located in Azure will be provisioned automatically, which means that the monitoring agent will be automatically installed. If you need to onboard Computers located on-premises, you need to install the agent manually. Follow the steps below to onboard non-Azure computers or VMs:

1. Open the **Azure portal** and sign in as a user who has Security Admin privileges.
2. In the left navigation, click **Security Center**.

3. In the Security Center left navigation under **General**, click the **Getting Started** option and click the **Get Started** tab.
4. Under **Add Non-Azure Computers**, click the **Configure** button, as shown in Figure 2-14.

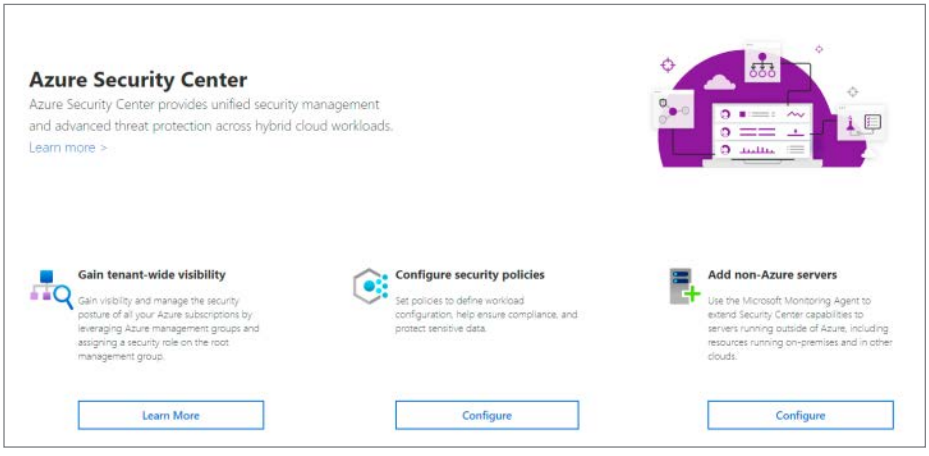


FIGURE 2-14 Option to onboard non-Azure computers

5. In the **Add New Non-Azure Computers** blade, select the workspace in which you want to store the data from these computers, and before onboarding any computers, make sure to click **Upgrade** to upgrade the Workspace to Azure Defender, as shown in Figure 2-15.

FIGURE 2-15 Upgrading the workspace to Azure Defender

6. If you don't see that the **Upgrade** button has changed to **Add Servers**, click the **Refresh** button and you should see the **Add Servers** button, as shown in Figure 2-16. Click it to proceed.

FIGURE 2-16 Adding servers to the workspace

7. Once you click this button, the **Agents Management** page appears, as shown in Figure 2-17.

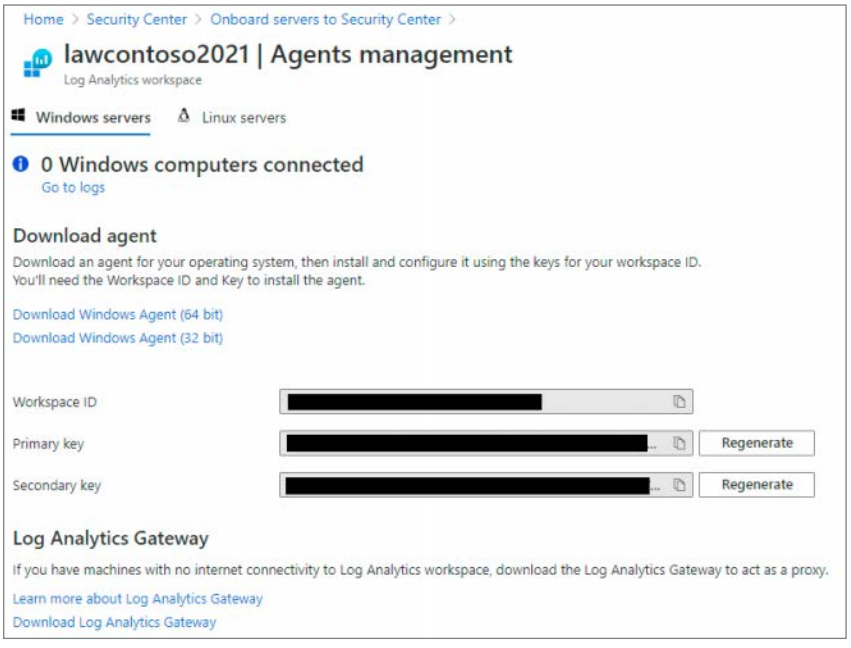


FIGURE 2-17 Agent selection

8. On this page, you should click the appropriate Windows agent (64- or 32-bit version), and if you are installing this in a Linux operating system, click the **Linux Servers** tab and follow the instructions from there. Make sure to copy the **Workspace ID** and **Primary Key** values to the clipboard. You will need those values when installing the agent in the target system.
9. When you finish downloading it, you can close the Security Center dashboard (close your browser) and copy the agent installation file to a shared network location where the client can access it.

For this example, the agent installation will be done in a Windows Server 2016 computer located on-premises. However, the same set of procedures apply to a non-Azure VM located in the cloud. Log in in the target system and follow the steps below to perform the installation:

1. Double-click the **MMASetup-AMD64.exe** file, and if the **Open File–Security Warning** dialog appears, click **Run**.
2. If the **User Access Control** dialog appears, click **Yes**.
3. On the **Welcome To The Microsoft Monitoring Agent Setup Wizard** page, click **Next**.
4. Read the **Microsoft License Terms**, and click **I Agree**.

5. On the **Destination Folder** page, leave the default selection and click **Next**. The **Agent Setup Options** page appears, as shown in Figure 2-18.

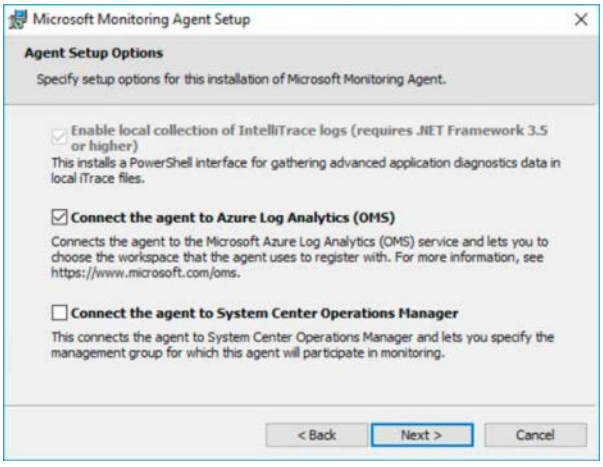


FIGURE 2-18 Selecting the target service

6. Select **Connect The Agent To Azure Log Analytics (OMS)**, as shown in Figure 2-18, and click **Next**. The **Azure Log Analytics** page appears, as shown in Figure 2-19.

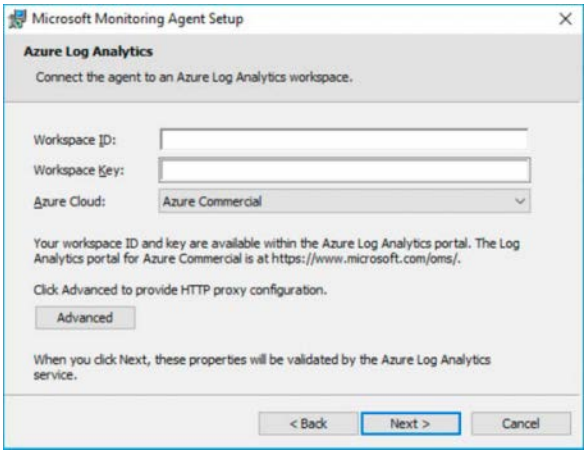


FIGURE 2-19 Providing the workspace ID and primary key

7. On this page, you need to write the Workspace ID and the Primary Key that were obtained in step 8 of the previous procedure. Notice that the Primary Key should be entered in the **Workspace Key** field. If this computer is behind a Proxy Server, you need to click the **Advanced** button and provide the Proxy URL and authentication if needed. Once you finish filling these options, click **Next**.
8. On the **Microsoft Update** page, select **Use Microsoft Update For Updates (Recommended)** and click **Next**.

9. On the **Ready To Install** page, review the **Summary** field and click **Install**.

   The **Installing The Microsoft Monitoring Agent** page appears, and the installation proceeds.

10. Once the installation is finished, the **Microsoft Monitoring Agent Configuration Completed Successfully** page appears. Click **Finish**.

You can also perform this installation using the command line interface (CLI) using the following code:

```
MMASetup-AMD64.exe /Q:A /R:N /C:"setup.exe /qn ADD_OPINSIGHTS_WORKSPACE=1 OPINSIGHTS_
WORKSPACE_AZURE_CLOUD_TYPE=0 OPINSIGHTS_WORKSPACE_ID=<yourworkspaceID> OPINSIGHTS_
WORKSPACE_KEY=<yourworkspaceprimarykey> AcceptEndUserLicenseAgreement=1"
```

IMPORTANT **The `/C` switch in this example uses IExpress as its self-extractor.**

Most of the parameters that you saw in the agent installation are self-explanatory; the only one that might not be readily apparent is `OPINSIGHTS_WORKSPACE_AZURE_CLOUD_TYPE`, which is the cloud environment specification. The default is `0`, which represents Azure commercial cloud. Only use `1` if you are installing the agent in an Azure government cloud.

It can take some time for this new non-Azure computer to appear in Security Center, but if you want to validate the connectivity between this computer and the workspace, you can use the `TestCloudConnection` tool. On the target computer, open the command prompt and navigate to the folder `\Program Files\Microsoft Monitoring Agent\Agent`. From there, execute the command `TestCloudConnection.exe`, and if the connectivity is working properly, you should see all tests followed by this message: `Connectivity test passed for all hosts for workspace id <workspace id>`.

Onboard resources from other cloud providers

After upgrading to Azure Defender, you will be able to use cloud connectors to connect to AWS or GCP. When connecting Security Center with AWS, you are integrating with AWS Security Hub, and the insights that are gathered from Security Hub will appear on the Security Center recommendations page. With GCP, Security Center integrates with the GCP Security Command, and you will also be able to see the insights in the Security Center recommendations.

For this example, you will connect AWS with Security Center. You will need to complete the following work on the AWS side before you start configuring Security Center:

- Enable AWS Config
- Enable AWS Security Hub
- Verify that there is data flowing to the Security Hub
- Configure AWS authentication, which can be done by creating the following:
  - An IAM role for Security Center
  - An AWS user for Security Center

- Regardless of the authentication method you selected previously, make sure that this role/user has the following permissions policies:
  - SecurityAudit
  - AmazonSSMAutomationRole
  - AWSSecurityHubReadOnlyAccess
- When configuring the Account ID in AWS, make sure to use the Microsoft Account ID 158177204117.

With those steps in place, you are ready to configure the cloud connector, but if you also want to onboard servers that are in AWS, you will need to ensure that the following tasks are done prior to configuring the cloud connector in Azure Security Center:

- Install the AWS Systems Manager on your servers (EC2 instances) that reside in AWS. For instructions, see *http://aka.ms/ascbookaws*.
- Configure this Server (EC2 Instance) to use Azure Arc. For instructions, see *http://aka.ms/ascbookarc*.
- In Azure, make sure to create a service principal that will be used for Azure Arc. Follow the steps found in this article to configure it: *http://aka.ms/ascbookspn*.

Now that all pre-requisites are fulfilled, you can follow the steps below to start the configuration of the AWS connector in Security Center:

1. Open **Azure portal** and sign in as a user who has ownership privileges in the subscription.
2. In the left navigation, click **Security Center**.
3. In the Security Center left navigation, under **Management**, click the **Cloud Connectors** option, and click the **Add AWS Account** button. The **Connect AWS Account** page appears, as shown in Figure 2-20.

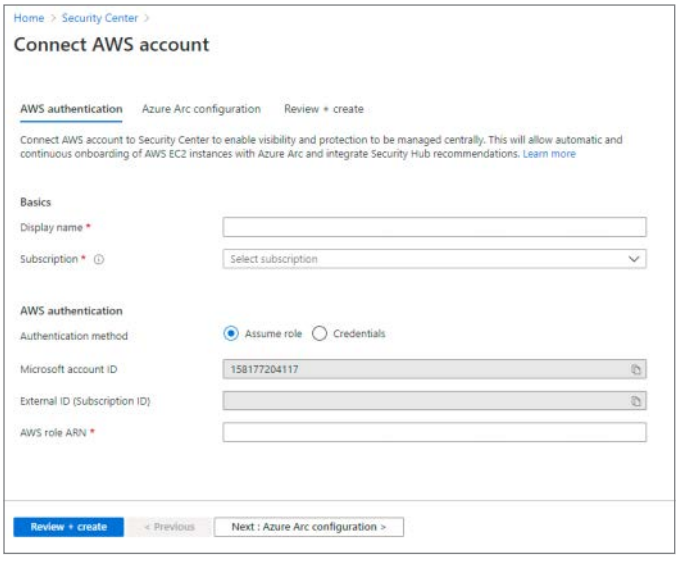


FIGURE 2-20 Connecting to AWS

4. In the **Basics** section, type a name for the connector and select the appropriate subscription from the drop-down menu.
5. In the **AWS Authentication** section, use the appropriate method (**Assume Role** if you created a role or **Credentials** if you created a user). Assuming that you used a role, the AWS role ARN number must be provided. This number is located in the summary of the role you created in AWS. Click the **Next Azure Arc Configuration** button, and the settings shown in Figure 2-21 appear.

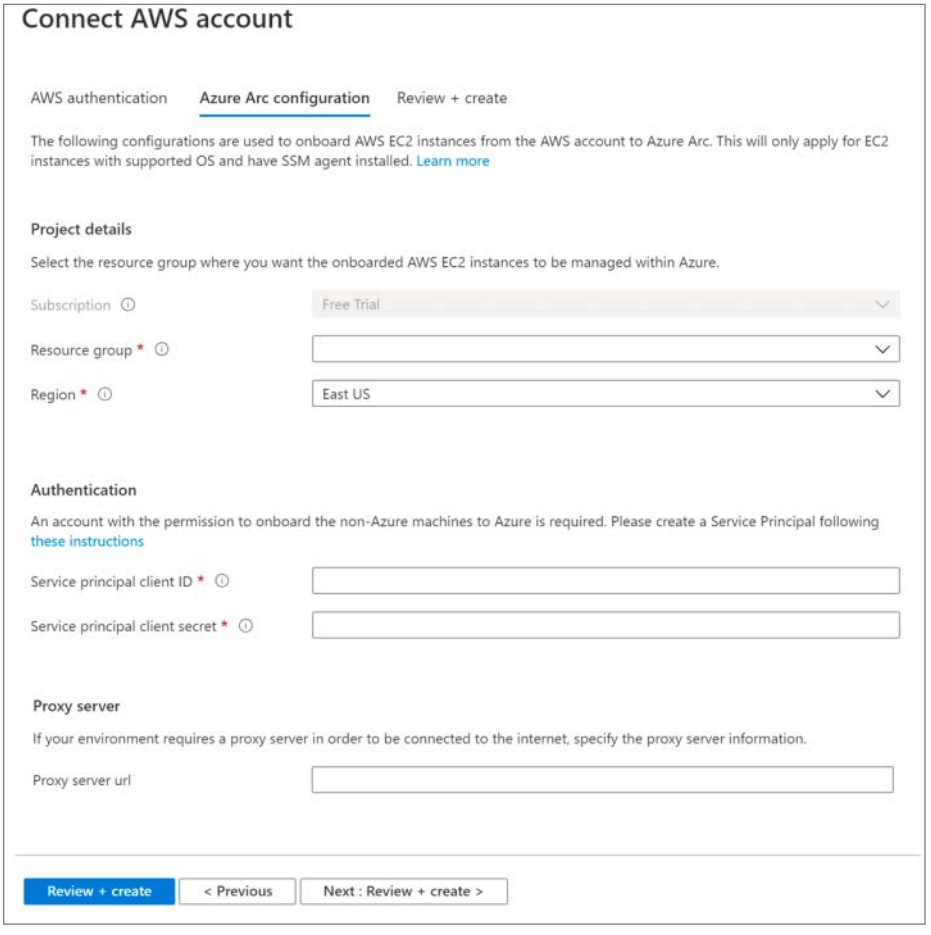


FIGURE 2-21 Configuring Azure Arc settings

6. Select the **Resource Group** and **Region**.
7. In the **Authentication** section, you need to provide the **Service Principal Client ID** and the **Client Secret**.

8. Click the **Review + Create** button and complete this operation.

   Once you finish, you will see the connector, as shown in Figure 2-22.

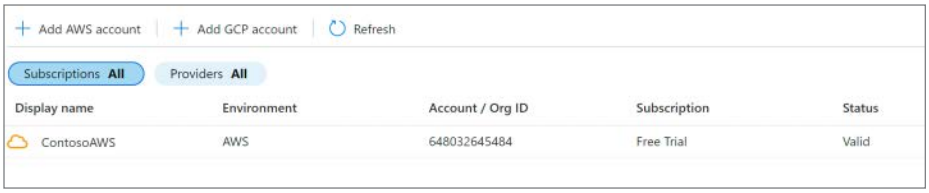


FIGURE 2-22 Configured AWS connector

After some time, you will be able to see recommendations for your AWS account. These recommendations will appear with the AWS tag, as shown in Figure 2-23.

FIGURE 2-23 Recommendations appear with the AWS tag.

At this point, your Azure Arc machines will be discovered, but you still need to install the Log Analytics agent on those machines, and there is a specific recommendation for that, as shown in Figure 2-24.

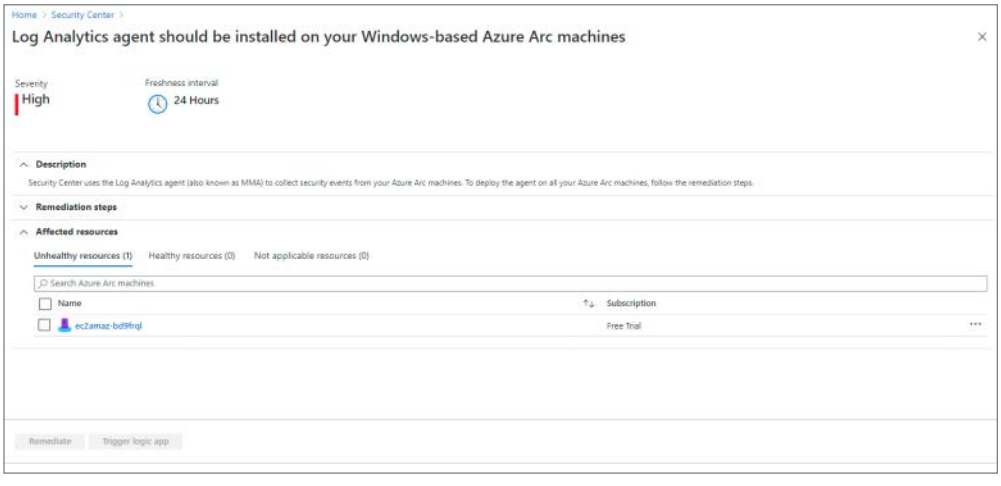


FIGURE 2-24 Recommendations to install the Log Analytics agent on the Azure Arc machine

You can leverage the **Quick Fix** feature to quickly deploy the agent to this Azure Arc machine. You just need to select the server and click the **Remediate** button. In Figure 2-24, the Freshness Interval indicates that it might take 24 hours for this remediation to take effect.

IMPORTANT **To onboard resources in Google Cloud Platform (GCP), follow the instructions here: *http://aka.ms/ascbookgcp*.**

Onboard resources using PowerShell

In large deployments, you might consider using Security Center PowerShell modules to help you quickly performing onboarding operations. To prepare the environment you must first install the `Az.Security` module using the commands below:

```
Set-ExecutionPolicy -ExecutionPolicy AllSigned
Install-Module -Name Az.Security -Force
```

When finished, use the `Connect-AzAccount` PowerShell command to log in to your Azure account. Next, register your subscriptions to the Security Center Resource Provider. Run the commands below, and make sure to replace the `<subscription ID>` field for your subscription number, which can be obtained using the command `Get-AzSubscription`.

```
Set-AzContext -Subscription "<subscription ID>"
Register-AzResourceProvider -ProviderNamespace 'Microsoft.Security'
```

At this point, you can start performing all operations that you need to onboard Security Center in your subscription. Usually, the first one is to upgrade from Free to Standard tier. First, you will set the context for the subscription that you want to upgrade, and then you perform the upgrade using the commands below:

```
Set-AzContext -Subscription "<subscription ID>"
Set-AzSecurityPricing -Name "default" -PricingTier "Standard"
```

You can use `Get-AzSecurityPricing` to verify if your subscription was correctly upgraded to the Standard version. If you already have a workspace and you want to connect Security Center to it, use the `Set-AzSecurityWorkspaceSetting` command. You will need the Workspace ID to perform this operation, which you can retrieve using the *`Get`*`-AzSecurityWorkspaceSetting` command. Another common operation to perform at this stage is to enable auto provisioning. For that, use the command below:

```
Set-AzSecurityAutoProvisioningSetting -Name "default" -EnableAutoProvision
```

To verify if the auto provisioning was correctly enabled, use the `Get-AzSecurityAuto ProvisioningSetting` command. One last operation we recommend is to configure the security contact information for email notifications. To configure this option, use the command below:

```
Set-AzSecurityContact -Name "YourName" -Email "youremailaddress" -Phone "yourphone"
-AlertAdmin -NotifyOnAlert
```

You can use the `Get-AzSecurityContact` command to verify your settings were configured properly. Make sure to visit the Azure Security Center community page to take advantage of many PowerShell samples: *https://github.com/Azure/Azure-Security-Center/tree/master/Powershell%20scripts*.

Inventory

After onboarding all resources from Azure and other cloud providers, you may want to list all resources available or query specific resources that you need more information about. You can use the **Inventory** feature in Security Center to accomplish that.

This feature uses Azure Resource Graph (ARG) in the background. ARG is an Azure service that provides the ability to query Security Center's data across multiple subscriptions using Kusto Query language. In a case where you want to query only resources that are available in AWS, you can easily create a resource type filter to see only those resources. Follow the steps below to access the Inventory feature and create this filter:

1. Open the **Azure portal** and sign in as a user who has read permission in the subscription.
2. In the left navigation, click **Security Center**.
3. In the Security Center left navigation, under **General**, click the **Inventory** option. The **Inventory** page appears, as shown in Figure 2-25.

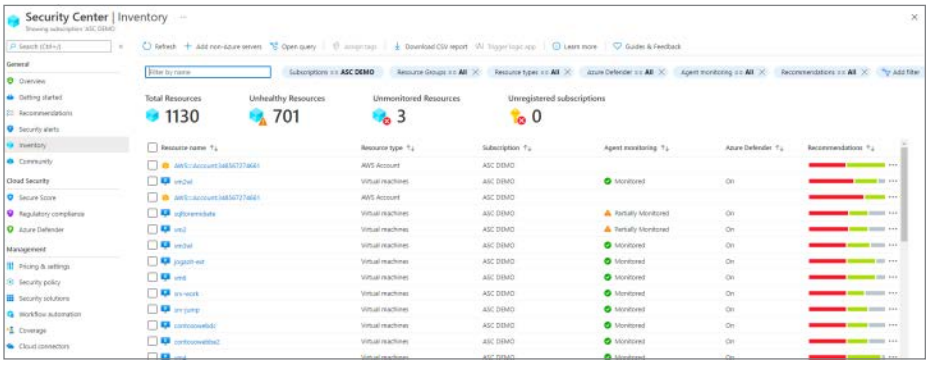


FIGURE 2-25 The Inventory page

4. Click the **Resource Types** filter, click **Select All** to uncheck all the items, and then only select **aws account** and **aws resources**, as shown in Figure 2-26.

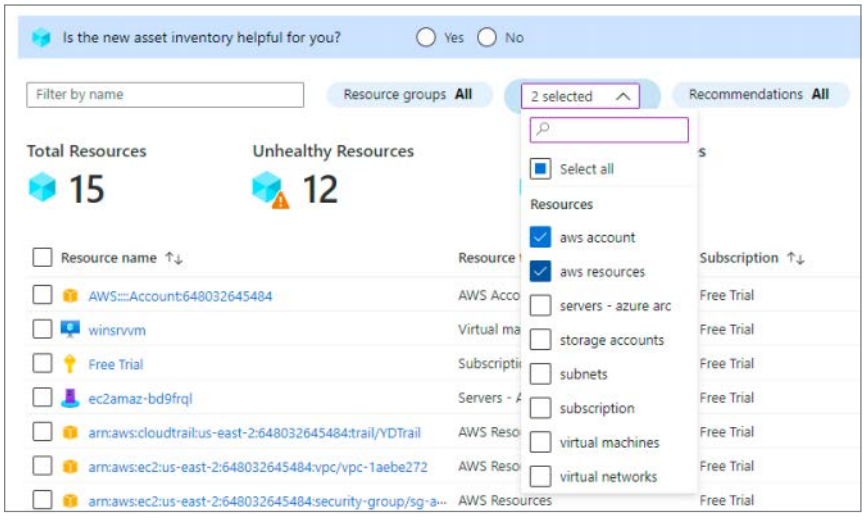


FIGURE 2-26 Filtering by resource types

5. After selecting those items, click outside the drop-down menu to commit the changes. At this point, you should see only your AWS resources/account.
6. After applying the filter, you can also select a particular resource from the list to see more details about that resource. The **Resource Health** page for the opened resource also presents the list of recommendations that are open, as shown in Figure 2-27.

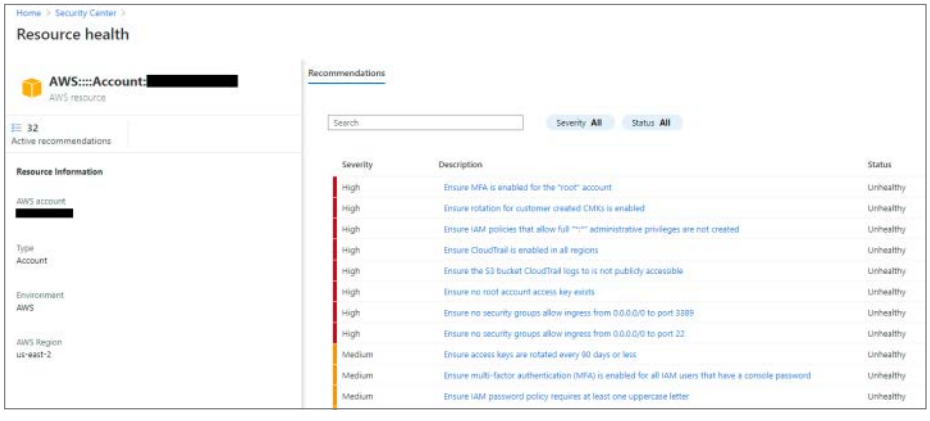


FIGURE 2-27 Filtering by resources types

Besides filtering on resource types, you can also create filters based on the following variables:

- Resource name
- Resource groups
- Recommendations
- Agent monitoring status
- Azure Defender status (on, off, or partially enabled)
- Security findings (including values from the vulnerability assessment)
- Tag

If you need to create filters that are beyond the options that are available, you can also customize your own query using ARG. You can create the base visualization using the filters that are available in the Inventory dashboard, and from there click the **Open Query** button, as shown in Figure 2-28.

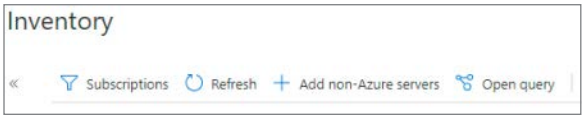


FIGURE 2-28 Accessing the ARG interface via the Open Query button

After you click this button, the **Azure Resource Graph Explorer** page appears, as shown in Figure 2-29.

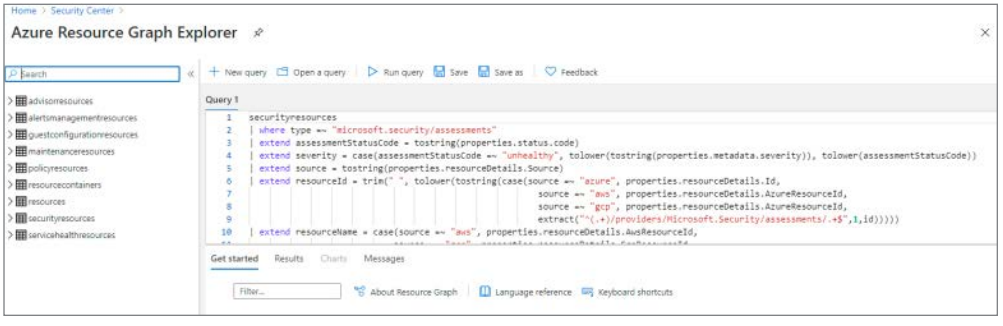


FIGURE 2-29 Azure Resource Graph Explorer with a pre-defined query

From this page, you can click **Run Query**, which will produce a similar result to what you have in the Inventory page since this query is based on the filtering that was configured on that page. Also, you can customize this query according to your own needs.

> ***NOTE*** **For other sample ARG queries, consult the Azure Security Center community page at *https://github.com/Azure/Azure-Security-Center/tree/master/Kusto/Azure%20Resource%20Graph*.**

Index

A

access
  and identity management, 10
  and permissions, 97–98
  preventing, 101
  requesting in JIT, 167–168
access control, 30
ACLs (access control lists), 13
ACR (Azure Container Registries), 134–137
Activity Log, 21
Adaptive Application Control, 175–181
Adaptive Network Hardening, 110–113
agents
  installing in Security Center, 36
  selecting in Security Center, 41
AKS (Azure Kubernetes Services), 5, 22, 103, 134–135
alerts. *See also* REST (Representational State Transfer) API
  accessing, 126–129
  accessing in Azure Sentinel, 189–192
  accessing using Graph Security API, 200–203
  activity evaluation prior to, 125
  in ARG (Azure Resource Graph), 131–132
  details page, 127
  overview, 124–126
  suppressing, 129–131
antimalware, 108–109, 144
antivirus protection, 108
API reference, accessing, 198
App Service, Azure Defender for, 137
ARG (Azure Resource Graph), 48–50, 131–132
ARM (Azure Resource Manager)
  and automation, 32
  Azure Defender for IoT, 144
  templates, 71, 198, 205–206, 210–213
artifacts and Blueprint definitions, 68–70
ASC (Azure Security Center)
  adding servers, 40
  addressing recommendations, 94–95
  agent selection, 41
  alerts, 25
  architecture, 25–28
  auto provisioning, 37–39
  automation, 32
  Azure Policy and management groups, 208–209
  Azure Security Benchmark, 76
  centralized management, 31
  compliance initiative, 78–81
  compliance reports, 76
  compute recommendations, 99–109
  Conditional Access policies, 97–98
  connecting with AWS, 43–46
  continuous export, 25
  Continuous Export feature, 25
  CSPM (Cloud Security Posture Management), 23
  customizing policies, 61–64
  CWPP (Cloud Workload Protection Platforms), 24
  dashboard, 29
  data and storage, 114–118
  Deny and Enforce effects, 66
  deployment scenarios, 23–24
  enabling MFA (multi-factor authentication), 95–98
  Free Tier option, 35
  incorporating, 32–34
  Initiative Compliance dashboard, 57
  installing agents, 36
  inventory, 48–50
  Linux systems, 26
  Log Analytics Agent, 25–27
  management at scale, 209–210
  Microsoft Antimalware, 108–109
  onboarding resources, 34–47
  overview, 24
  planning adoption, 30–34

ASC (Azure Security Center) (*continued*)
policies, 57–64
PowerShell, 47–48
recommendations, 25, 32
regulatory compliance, 74–78
roles and permissions, 30
security assessments, 115
Security Controls, 95
and Sentinel workspace, 31
storage, 31
subscription coverage, 34–35
subscription ownership, 98
subscription status, 34–35
upgrading to Azure Defender, 24
VMs (virtual machines), 39–43
Windows systems, 26
assume breach mentality, adopting, 7
attack surface, reducing, 161. *See also* threat hunting
authorization and authentication, 12–13
auto provisioning, Security Center, 37–39
AWS (Amazon Web Services), 24, 43–46
Azure Activity Log, 21
Azure AD (Active Directory), 19
Azure Arc, 140
Azure Blueprints, large-scale provisioning with, 68–71
Azure Cloud Services, recommendations, 103
Azure Defender. *See also* Defender Antivirus
alerts, 124–132
analytics, 28
for App Service, 137
for ARM (Azure Resource Manager), 144
for Azure Storage, 19
for containers, 134–137
for DNS, 145–146
for Key Vault, 143
overview, 123–124
pricing tiers, 104–105
Qualys VA solution, 105–106
security incident, 148
for servers, 132–133
for SQL, 139–143
for storage, 138
threat detection, 27
upgrading to, 24
workloads, 36
Azure Defender for IoT
configuring, 153–159
and CyberX, 158–160
overview, 149–152
Azure Disk Encryption, 17
Azure Identity Protection, 19
Azure Monitor Workbooks, 34
Azure Policy. *See also* policies
audit mode, 53
components, 52
definitions and assignments, 52
DINE (`deployifnotexists`) mode, 53
exemptions, 54–56
importance of, 207–208
initiative definitions, 52
overview, 51–56
Security Center and management groups, 208–209
Azure Security. *See also* security
container security, 21–22
Identity Protection, 19
logging, 20–21
network protection, 14–17
overview, 12–13
storage protection, 17–19
VM protection, 13–14
Azure Security Benchmark, 76
Azure Security Center
adding servers, 40
addressing recommendations, 94–95
agent selection, 41
alerts, 25
architecture, 25–28
auto provisioning, 37–39
automation, 32
Azure Policy and management groups, 208–209
Azure Security Benchmark, 76
centralized management, 31
compliance initiative, 78–81
compliance reports, 76
compute recommendations, 99–109
Conditional Access policies, 97–98
connecting with AWS, 43–46
continuous export, 25
Continuous Export feature, 25
CSPM (Cloud Security Posture Management), 23
customizing policies, 61–64
CWPP (Cloud Workload Protection Platforms), 24
dashboard, 29
data and storage, 114–118
Deny and Enforce effects, 66
deployment scenarios, 23–24
enabling MFA (multi-factor authentication), 95–98
Free Tier option, 35

incorporating, 32–34
Initiative Compliance dashboard, 57
installing agents, 36
inventory, 48–50
Linux systems, 26
Log Analytics Agent, 25–27
management at scale, 209–210
Microsoft Antimalware, 108–109
onboarding resources, 34–47
overview, 24
planning adoption, 30–34
policies, 57–64
PowerShell, 47–48
recommendations, 25, 32
regulatory compliance, 74–78
roles and permissions, 30
security assessments, 115
Security Controls, 95
and Sentinel workspace, 31
storage, 31
subscription coverage, 34–35
subscription ownership, 98
subscription status, 34–35
upgrading to Azure Defender, 24
VMs (virtual machines), 39–43
Windows systems, 26
Azure Sentinel
integration with, 186–192
overview, 184–186
and Security Center workspace, 31
Azure Storage Service Encryption, 18
Azure Virtual Networks (VNet), 101

B

botnet, 3
breaches. *See* assume breach mentality
Brno University Hospital, 2
Brownfield devices, 159
brute-force attacks, 99–100, 161
BYOD (bring-your-own-device) models, 5

C

CAV (counter-antivirus) services, 2
centralized management, 31
China, IP-address attacks from, 7
CIS (Center for Internet Security), 14
cloud providers, onboarding resources from, 43–47
cloud threats and security, 7–12
CNI (container network interface) plug-in, 21
code files, downloading, xviii
code injection, 2
compliance, cloud threats and security, 9–10
compute recommendations, secure management ports, 99–102
Compute security, 13. *See also* security
Conditional Access policies, 97–98. *See also* policies
configuration, flaws in, 8
container security, 21–22
container security, recommendations, 107
Contoso-Linux-VM machine, 99
COVID-19, 1, 5, 161
credential phishing flow, 3
CSP (cloud solution providers), 9–10
CSPM (Cloud Security Posture Management), 23, 32–34
CWPP (Cloud Workload Protection Platforms), 8, 24
cyber kill chain
and fusion alerts, 146–148
overview, 3–7
cybercrime, 1–3

D

data
isolating, 28
and storage, 114–118
data aggregation, Azure Sentinel, 189
data protection, cloud threats and security, 11–12
DDoS attacks, protecting against, 15–17
Defender Antivirus, 108. *See also* Azure Defender
deployment scenarios, 23–24
diagnostics logs, 20
dictionary attacks, 99
Disk Encryption, 17
DLL (Dynamic Link Library) attack, 3
DNS, Azure Defender for, 145–146
domain dominance, 4
downloading. *See also* drive-by download sites
code files, xviii
Microsoft Digital Defense Report, 2
drive-by download sites, 5. *See also* downloading

E

EDR (endpoint detection and response) solution, 11
email phishing, 2–3
email recipients, security contacts as, 121
encryption, 18
endpoint protection
  cloud threats and security, 11
  enabling, 108–109
Ericsson study about IoT devices, 149

F

Fender, Sarah, 201
FIM (file integrity monitoring), 168–174
firewall, 18
Free Tier option, subscriptions, 35
fusion alerts and cyber kill chain, 146–148

G

Gartner CFO Survey, 161
GCP (Google Cloud Platform), 24, 43
geolocation, basing workspace organization on, 28
GitHub
  community, 186
  repository, 198
  scanning by bots, 8–9
Graph Security API, using to access alerts, 200–203
Greenfield devices, 159

H

HTTP GET request, 197–198
Hyper-V virtualization platform, 14

I

IaC (Infrastructure as Code), 205
identity and access management, 10
Identity Protection, 19
identity-based attacks and passwords, 96
InfoSec Institute, 6
integration, simplifying, 201
Interpol report (2020), 1
inventory, Security Center, 48–50
investigation visualization, 186
IoT
  and Azure Defender, 149–153
  configuring for Azure Defender, 153–159
  and CyberX, 158–160
  Hub service, 150
  security, 151
IoT devices, statistic about, 149
IP addresses, attacks from, 7
ISO27001 standard, 73
isolating data, 28

J

JIT (just-in-time) VM access, 161–168. *See also* VMs (virtual machines)
JSON and policy definitions, 71
JSON content, accessing, 21
JSON HTTP GET request, 197–198

K

Kemnetz, John, 184
Key Vault, Azure Defender for, 143
key-management, 18
Korea, IP-address attacks from, 7
KQL (Kusto Query Language), 190, 192
Kubernetes, 5, 22, 103, 134–135

L

Linux files, adding to FIM, 172
Linux systems
  Azure Defender Server for, 133
  Security Center, 26
Log Analytics Agent, 25–27, 99, 102–103
logging, 20–21
Logic App, 119, 121–122
lurking, 6

M

Machado de Wright, Laura, 186
management at scale
  best practices, 209–210
  cornerstones, 205–209
  importance of, 205
management ports, security of, 99–102
MFA (multi-factor authentication), 58, 87, 95–98
Microsoft Antimalware, 108–109
Microsoft Defender Antivirus, 108
Microsoft Digital Defense Report (2020), 1–2, 5
ML (machine learning) models and Azure Sentinel, 185–186

N

Network Map, displaying, 110–112
network protection, 14–18
networking. *See also* virtual networks
  Adaptive Network Hardening, 110–113
  overview, 109
Nick, Ben, 191
NICs (network interface cards), 101
Nitol botnet, 3
NSGs (network security groups), 13, 22, 101, 112

O

onboarding resources
  auto provisioning, 37–39
  overview, 34–36
  virtual machines, 39–43
operational security, 10. *See also* security

P

Palo Alto Networks report, 8
passwords and identity-based attacks, 96, 99
PCI DSS (Payment Card Industry Data Security Standard), 73–75
pentest exercise, dismissing alerts during, 129
permissions
  and access, 97–98
  and roles, 30
phishing attacks, 2–3, 5
pillars of security posture, 6
Pliskin, Ram, 137
pods and containers, 21
policies. *See also* Azure Policy; Conditional Access policies
  for Adaptive Network Hardening, 113
  customizing, 61
  deny effects, 72
  deployment and best practices, 71–72
  enforcement and governance, 64–71
  monitoring and implementation, 64
  overriding settings, 71–72
  Security Center, 57–61
ports, managing for JIT, 164–165
PowerShell
  and ARM templates, 210
  and Azure Defender, 133
  and Azure Sentinel, 189–190
  and JIT VM Access policy, 168
  and policy deployment, 71
  using to onboard resources, 47–48
privileged access, securing, 11
protect-detect-respond pillars, 6
provisioning with Azure Blueprints, 68–71
public secret attack scenario, 9

R

ransomware, 2, 5
RBAC (Role-Based Access Control), 12, 30–31
RDP (Remote Desktop Protocol) brute force, 5, 13, 161
recommendations
  addressing, 94–95
  and controls focused on compute, 99–109
  data and storage, 114–118
  MFA (multi-factor authentication), 95–98
  networking, 109–113
  remediating, 118–122
  Security Center, 32
registry. *See* Windows registry
regulatory standards and compliance, 73–81
remediation, automation of, 186
REST (Representational State Transfer) API. *See also* alerts
  overview, 195–196
  using to access alerts, 196–200
restrictions, creating, 175
risk management, cloud threats and security, 10
roles and permissions, 30

S

Secure Score
automations, 90–93
calculation of, 64–65, 106
continuous export, 90–92
data, 90–92
decrease notification, 93
getting data, 90–92
MFA solutions, 87
Over Time report, 92–93
over time report, 92–93
overview, 83–89
resource exemptions, 87–89
security. *See also* Azure Security; Compute security; operational security
and cloud threats, 7–12
of management ports, 99–102
managing reactively, 65–66
preventing misconfigurations, 66–67
security alerts. *See also* REST (Representational State Transfer) API
accessing, 126–129
accessing in Azure Sentinel, 189–192
accessing using Graph Security API, 200–203
activity evaluation prior to, 125
in ARG (Azure Resource Graph), 131–132
details page, 127
overview, 124–126
suppressing, 129–131
Security Center
adding servers, 40
addressing recommendations, 94–95
agent selection, 41
alerts, 25
architecture, 25–28
auto provisioning, 37–39
automation, 32
Azure Policy and management groups, 208–209
Azure Security Benchmark, 76
centralized management, 31
compliance initiative, 78–81
compliance reports, 76
compute recommendations, 99–109
Conditional Access policies, 97–98
connecting with AWS, 43–46
continuous export, 25
Continuous Export feature, 25
CSPM (Cloud Security Posture Management), 23
customizing policies, 61–64
CWPP (Cloud Workload Protection Platforms), 24
dashboard, 29
data and storage, 114–118
Deny and Enforce effects, 66
deployment scenarios, 23–24
enabling MFA (multi-factor authentication), 95–98
Free Tier option, 35
incorporating, 32–34
Initiative Compliance dashboard, 57
installing agents, 36
inventory, 48–50
Linux systems, 26
Log Analytics Agent, 25–27
management at scale, 209–210
Microsoft Antimalware, 108–109
onboarding resources, 34–47
overview, 24
planning adoption, 30–34
policies, 57–64
PowerShell, 47–48
recommendations, 25, 32
regulatory compliance, 74–78
roles and permissions, 30
security assessments, 115
Security Controls, 95
and Sentinel workspace, 31
storage, 31
subscription coverage, 34–35
subscription ownership, 98
subscription status, 34–35
upgrading to Azure Defender, 24
VMs (virtual machines), 39–43
Windows systems, 26
security contacts, using as email recipients, 121
Security Controls, 95
Security Defaults, 97–98
security incident, Azure Defender, 148
security operations (SecOps), 32–33
security posture, building, 5–7
security recommendations, remediating, 118–122
servers
adding to workspace, 40
Azure Defender for, 132–133
SIEM (security information and event management)
integration with, 192–194
overview, 183–184
SLA (service-level agreement), 10
SOC (security operations center), 33–34

Solorigate attack, 3
Splunk, features of, 194
SQL, Azure Defender for, 139–143
SQL databases, sensitive data in, 116–118
SQL Server, enabling auditing on, 115–116
SSE (Storage Service Encryption), 18
SSH brute-force attacks, 161
SSH management port, exposure of, 99
storage
  Azure Defender for, 138
  and data, 114–118
  firewall, 18
  protection, 17–19
  Security Center, 31
streaming logs to SIEM, 183–184
subscription ownership, 98
supply chain attacks, 3
system updates, applying, 102–103

T

templates. *See* ARM (Azure Resource Manager)
threat detection, 124
  Azure Defender, 27
  methods of, 124
threat hunting, 191. *See also* attack surface
threats, common examples of, 5
TLS (transport layer security), 11
Trigger Logic App capability, 120

U

United States, IP-address attacks from, 7
updates, applying to system, 102–103
username/password lists, problem with, 99

V

Verizon Data Breach Report (2020), 5
VHD file format, 17
Vij, Anupam, 17
virtual networks, 14–16, 109–113. *See also* networking
VMBA (Virtual Machine Behavioral Analysis), 124
VMs (virtual machines). *See also* JIT (just-in-time) VM access
  determining health of, 163
  onboarding, 39–43
  protecting, 13–14
VMware virtualization platform, 14
VSCode (Visual Studio Code), creating ARM templates, 211–213
vulnerabilities, remediating, 104–106
Vulnerability Assessment dashboard, accessing, 142

W

Windows registry
  adding to FIM, 170
  visualizing changes to, 173–174
Windows systems
  Azure Defender Server for, 133
  Security Center, 26
Workflow Automation feature, 34
workflow automation, using to remediate recommendations, 118–122
workspace organization, basing on geolocation, 28