Microsoft 365 Security Administration

Exam Ref MS-500

Ed Fisher
Nate Chamberlain

Microsoft

Exam Ref MS-500 Microsoft 365 Security Administration

Ed Fisher
Nate Chamberlain

Exam Ref MS-500 Microsoft 365 Security Administration

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

ISBN-13: 978-0-13-580264-9
ISBN-10: 0-13-580264-4

Library of Congress Control Number: 2020942705

ScoutAutomatedPrintCode

CREDITS

EDITOR-IN-CHIEF
Brett Bartow

EXECUTIVE EDITOR
Loretta Yates

SPONSORING EDITOR
Charvi Arora

DEVELOPMENT EDITOR
Rick Kughen

MANAGING EDITOR
Sandra Schroeder

PROJECT EDITOR
Tracey Croom

COPY EDITOR
Rick Kughen

INDEXER
Cheryl Lenser

PROOFREADER
Sarah Kearns

TECHNICAL EDITORS
Ed Fisher, Bryan Lesko

EDITORIAL ASSISTANT
Cindy Teeters

COVER DESIGNER
Twist Creative, Seattle

GRAPHICS
TJ Graham Art

I dedicate this book to my wife, Connie, without whom this could not have happened and would not have mattered. Thanks for being my better half in every way. And to my fellow TSs with whom I share the best role at Microsoft.

—Ed Fisher

This page intentionally left blank

Contents at a glance

This page intentionally left blank

Contents

About the Authors

Ed Fisher, Security & Compliance Architect at Microsoft, focuses on all aspects of security and compliance within Office 365, especially Microsoft Threat Protection. He has spent nearly a decade helping Microsoft customers and partners succeed with Microsoft cloud and productivity solutions. You can learn more at *https://aka.ms/edfisher*.

Nate Chamberlain is a Microsoft 365 Certified Enterprise Administrator Expert. He has been an Office Apps and Services MVP since 2019, frequently blogging at *NateChamberlain.com* and speaking at Microsoft-focused events and user groups.

Acknowledgments

I'd like to express my deep gratitude to the following people, without whom this book would not have been possible.

Thank you to Loretta for bringing me into this project. Your patience is greatly appreciated! Thank you, Rick, for painstakingly editing every corner of this book to make it a better reading experience. Thanks to Bryan for all the early work and assistance. Thanks to Nate for coming in at the eleventh hour to bring this thing home. Thanks to Charvi for taking care of all the details that keep everything on track. Thanks to Greg for greenlighting this side hustle. Finally, thank you to all the people at Microsoft Press who worked so hard to create this book from the digital manuscript.

—Ed Fisher

I'm grateful to the hard-working team behind this book who brought me on board with Ed to write this guide and continually helped us make it the best it can be all the way to the press. Professional and personal growth are dear topics to me, and it's an honor of mine to be able to be part of this project, ultimately helping tech professionals gain their next certifications.

I also want to acknowledge the amazingly supportive and encouraging MVP community, as well as everyone out there who attends local and larger conferences and gets involved in user groups and professional networks. Time is always in short supply, and energy is limited. Making the decision to spend both time and energy in pursuit of community and growth is commendable, and I wish you the best in your ongoing endeavors.

—Nate Chamberlain

Introduction

The purpose of the MS-500 exam is to test your comprehension and practical ability when working with security and compliance features across Microsoft 365 and Azure. The exam includes high-level concepts that apply across all of Microsoft 365 to important concepts that are specific to a particular app or service. Like the exam, this book is geared toward giving you a broad understanding of Microsoft 365 Security Administration, as well as many common services and components on a more granular level.

While we've made every effort possible to make the information in this book accurate, Microsoft 365 is rapidly evolving, and there's a chance that some of the screens shown are slightly different now than they were when this book was written. It's also possible that other minor changes have taken place, such as minor name changes in features and so on.

This book covers every major topic area found on the exam, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions, and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. In many cases, we've provided links in the "More Info" sections of the book, and these links are a great source for additional study.

Organization of this book

This book is organized by the "Skills measured" list published for the exam. The "Skills measured" list is available for each exam on the Microsoft Learning website: *http://aka.ms/examlist*. Each chapter in this book corresponds to a major topic area in the list, and the technical tasks in each topic area determine a chapter's organization. Because the MS-500 exam covers four major topic areas, this book contains four chapters.

Preparing for the exam

Microsoft certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. We recommend that you augment your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Exam Ref and another study guide for your "at home" preparation and take a Microsoft Official Curriculum course for the classroom experience. Choose the combination that you think works best for you.

Note that this Exam Ref is based on publicly available information about the exam and the authors' experiences. To safeguard the integrity of the exam, authors do not have access to the live exam.

Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

Quick access to online references

Throughout this book are addresses to webpages that the authors have recommended you visit for more information. Some of these links can be very long and painstaking to type, so we've shortened them for you to make them easier to visit. We've also compiled them into a single list that readers of the print edition can refer to while they read.

Download the list at *https://MicrosoftPressStore.com/ExamRefMS500/downloads*.

The URLs are organized by chapter and heading. Every time you come across a URL in the book, find the hyperlink in the list to go directly to the webpage.

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/ExamRefMS500/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 *https://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*.

This page intentionally left blank

CHAPTER 2

Implement and manage threat protection

This chapter is all about Microsoft Threat Protection and includes five objectives. They address how to protect a hybrid organization, how to protect devices, how to protect applications, and how to protect the SaaS applications and data within Office 365.

Skills in this chapter:

- Skill 2.1: Implement an enterprise hybrid threat protection solution
- Skill 2.2: Implement device threat protection
- Skill 2.3: Implement and manage device and application protection
- Skill 2.4: Implement and manage Office 365 ATP
- Skill 2.5: Implement Azure Sentinel for Microsoft 365

Skill 2.1: Implement an enterprise hybrid threat protection solution

Enterprise hybrid threat protection is about addressing the challenges facing an organization with applications and identities that are served from both on-premises infrastructure and cloud solutions, such as Office 365. Identity is the new security boundary, and the goals of this objective are detecting when attempts are made to compromise identities, as well as ensuring authenticated users are not abusing their access.

This skill covers how to:

- Planning an Azure Advanced Threat Protection (ATP) solution
- Install and configure Azure ATP
- Manage Azure ATP Workspace Health
- Generate Azure ATP reports
- Integrate Azure ATP with Microsoft Defender ATP
- Manage suspicious activities

Planning an Azure Advanced Threat Protection (ATP) solution

Azure ATP requires some pre-work in order to successfully deploy, including ensuring that your domain controllers meet the hardware requirements, have the necessary software prerequisites installed, and have the required connectivity to Azure ATP endpoints in the cloud.

Capacity planning

You need to download and run the Azure ATP Sizing tool, TriSizingTool.exe, from Microsoft and run it from a workstation or server that can connect to all domain controllers in your environment. Doing so will evaluate the CPU utilization, available RAM, and network I/O, and it will make recommendations where more hardware needs to be added to domain controllers that are to run the Azure ATP agent.

The minimum hardware recommendations include:

- **CPU.** At least two cores.
- **RAM.** At least 6GB.
- **Disk space.** A minimum of 5GB free and at least 10GB free is recommended.

Those are really the bare minimums, and if your Active Directory has a larger number of objects, you should expect to need more. For the best performance, your domain controllers should have enough RAM to cache the entire NTDS.DIT in memory on top of the operating system requirements and any other software running on the domain controllers, so it is common for the Azure ATP Sizing tool to recommend more RAM.

If you cannot run the Azure ATP Sizing tool, there is a manual method you can use to estimate hardware needs, which is documented at *https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning#manual-sizing*, but you really should use the tool to automate this process.

> ***REAL WORLD*** **VIRTUALIZED DOMAIN CONTROLLERS AND MEMORY**
>
> **It's common to find domain controllers running as guests of a hypervisor host and with dynamically allocated memory. If that is the case in your environment, expect the sizing tool to report that these domain controllers will all need additional RAM. While it's always recommended that domain controllers be provisioned with a fixed RAM assignment, it is a requirement when running Azure ATP. Allocate a fixed amount of RAM or deploy the standalone agent, which also requires a fixed allocation of RAM. You may choose to try running with less RAM than the sizing tool calls for and increase the allocation of memory until you find what works in your environment. Just keep in mind that if there is not enough RAM on the domain controller, you may miss events. This means you should try to quickly dial in to what works for you.**

If the tool identifies domain controllers that require more resources than you have available to allocate, you can consider deploying Azure ATP using the Azure ATP Standalone deployment. With this approach, you deploy one or more additional servers that will run the Azure

ATP Standalone agent and you mirror (span) the network switch port for your domain controllers to a monitor interface on the Azure ATP Standalone server. One Azure ATP Standalone server can monitor multiple domain controllers in this way, as long as network traffic from all the domain controllers does not exceed the capacity of the Standalone server, which is estimated at 100,000 packets per second. This out-of-band deployment makes it harder for an attacker to determine that they are being watched, but it comes with the additional costs of deploying more servers.

EXAM TIP

Deploying the Azure ATP Standalone sensor has pros and cons. The pros include not needing to deploy additional software to domain controllers to upgrade their hardware and that the out-of-band deployment can make it harder for an adversary to detect. The cons include the additional cost, the need for a mirror port, and that you lose the ability to directly capture ETW events on the domain controller, which are necessary for certain detections, including LDAP-based reconnaissance. You can get around this by configuring event forwarding from domain controllers to the standalone sensor, but that does increase the complexity of your deployment.

Prerequisites

The Azure ATP agent can be installed on domain controllers, including RODCs, running the following operating systems:

- Server 2008 R2 SP1 (not including Server Core)
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016 (including Windows Server Core but not Windows Nano Server)
- Windows Server 2019 (including Windows Core but not Windows Nano Server)

Server 2019 requires that KB4487044 be installed. In all cases, .Net Framework 4.7 will be installed if it is not already present and might require a reboot.

The Azure ATP standalone agent can be installed on servers running the following operating systems:

- Windows Server 2012 R2
- Windows Server 2016 (including Server Core) single standalone agent can be used to monitor multiple domain controllers, assuming that there is sufficient hardware, and the network switch supports mirroring traffic from multiple ports and can be used to monitor domains with a functional level of 2003 or later. The server running the standalone agent can be domain-joined or it can run in workgroup mode. If it is in workgroup mode, ensure that time synchronization is set up with the domain(s) to monitor.

It should have at least two network interface cards. One will be used for management, while the other will be connected to the span port, so it can monitor network traffic for the domain controller(s).

You also need to ensure that all domain controllers or standalone agents that you will deploy have Internet connectivity to the appropriate Azure endpoints. If you are using a proxy server or other web filtering solution, permit connectivity to the endpoints documented at *https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-proxy*.

See Table 2-1 for an overview of the required endpoints.

TABLE 2-1 Azure ATP service endpoints

Service Location	*.atp.azure.com DNS Record
US	*triprd1wcusw1sensorapi.atp.azure.com* *triprd1wcuswb1sensorapi.atp.azure.com* *triprd1wcuse1sensorapi.atp.azure.com*
Europe	*triprd1wceun1sensorapi.atp.azure.com* *triprd1wceuw1sensorapi.atp.azure.com*
Asia	*triprd1wcasse1sensorapi.atp.azure.com*

Install and configure Azure ATP

Installing and configuring Azure ATP involves connecting to the portal, providing information for your set up, downloading the installation package, and deploying it to the servers.

The Azure ATP portal

When you sign in to the portal for the first time, you will create the instance of Azure ATP for your environment. You will be prompted for the username (NetBIOS format), password, and Active Directory domain name for the service account you will use; this account should be a user account with Read-Only access to your environment. Once you enter the information, you can download the sensor setup file. This zip file will install either the Azure ATP agent on a domain controller or the Azure ATP Standalone agent on a non-domain controller, and it contains the installer and a configuration file. You will also have to copy the Access key, which is used to establish the initial connection to your Azure ATP instance. Once installed, all authentication is through certificates.

Azure ATP supports RBAC through three built-in security groups. To access the Azure ATP console, a user must be a member of at least one of these groups. At the time of this writing, custom RBAC is not available. The built-in roles are listed in Table 2-2.

TABLE 2-2 Azure ATP roles and capabilities

Capability	Azure ATP Administrators	Azure ATP Users	Azure ATP Viewers
Log in to the portal	Yes	Yes	Yes
Modify security alert status	Yes	Yes	No
Export security alerts	Yes	Yes	Yes
Download reports	Yes	Yes	Yes

Modify monitoring alert status	Yes	No	No
Modify Azure ATP configuration	Yes	No	No
Modify data sources	Yes	No	No
Modify updates	Yes	No	No
Modify scheduled reports	Yes	Yes	No
Modify tags	Yes	Yes	No
Modify exclusions	Yes	Yes	No
Modify language	Yes	Yes	No
Modify notifications	Yes	Yes	No
Modify detections	Yes	Yes	No
View profiles and alerts	Yes	Yes	Yes

Membership in the Azure ATP RBAC groups is managed through the Groups Management blade in the Azure Active Directory portal, as shown in Figure 2-1.

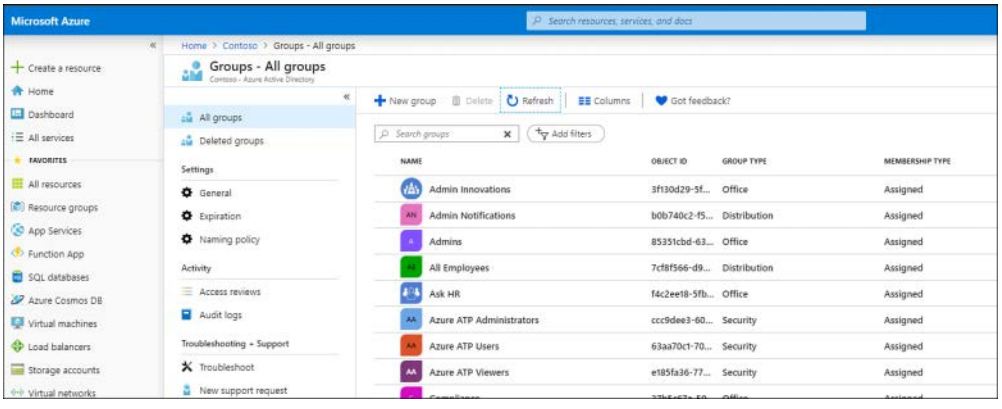

FIGURE 2-1 Azure Groups showing the Azure ATP security groups

EXAM TIP

Any user who is a Global Administrator or a Security Administrator is automatically an Azure ATP Administrator.

Manage Azure ATP Workspace Health

The Azure ATP portal includes a section on Workspace Health, where issues such as connectivity, disconnected sensors, or service account authentication are reported. The Health icon shown in Figure 2-2 will indicate whether there is any detected problem by displaying a red dot over the icon.

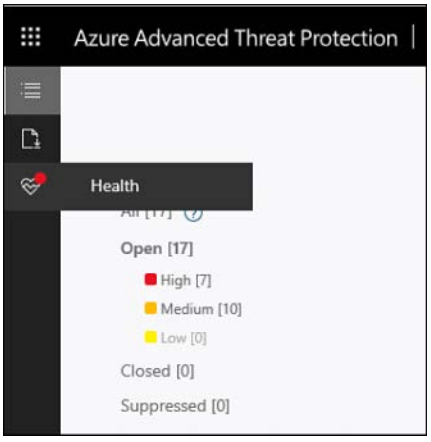

FIGURE 2-2 The Azure Advanced Threat Protection menu indicating a problem with Workspace Health

To access Workspace Health and view the issue, simply click the icon. Workspace Health will list the problem or problems detected and provide information on how to correct the issue. It's important to check this to see if an agent is no longer reporting or if the account used by the service can no longer authenticate; you should remediate any problems immediately.

Generate Azure ATP reports

The Reports page in the Azure ATP portal lets you download four report types:

- **Summary.** This is a summary of alerts and health issues.
- **Modifications To Sensitive Groups.** Every modification to sensitive groups in Active Directory, including modifications that generated an alert.
- **Passwords Exposed In Cleartext.** All LDAP authentications that exposed user passwords in cleartext.
- **Lateral Movements Paths To Sensitive Accounts.** Sensitive accounts at risk of being compromised through lateral movement techniques.

By default, the report will show the last seven days' data, but you can use the calendar selector to configure a custom date range. Reports are downloaded as Excel files. You can also schedule any of the reports on a Daily, Weekly, or Monthly basis and at a specific time, as shown in Figure 2-3.

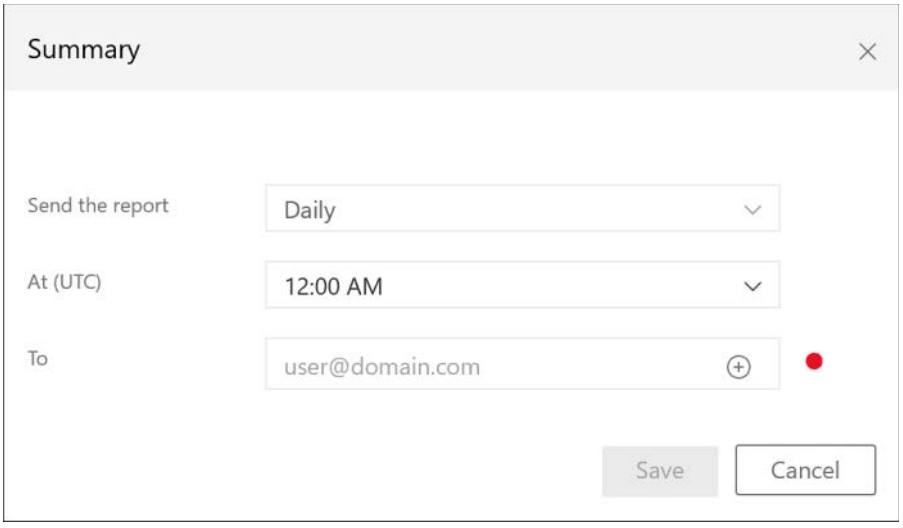

FIGURE 2-3 Scheduling Azure ATP reports in the portal

Integrate Azure ATP with Microsoft Defender ATP

Azure ATP can integrate with Microsoft Defender ATP, integrating the UEBA capabilities on domain controllers with EDR capabilities on endpoints to enhance the protections provided by both. To enable this integration, you must do so in both the Azure ATP portal, and the Microsoft Defender ATP Security Center.

In the Azure ATP portal, under **Configuration**, simply switch the **Integration With Windows Defender ATP** slider to **On** and select **Save**, as shown in Figure 2-4.

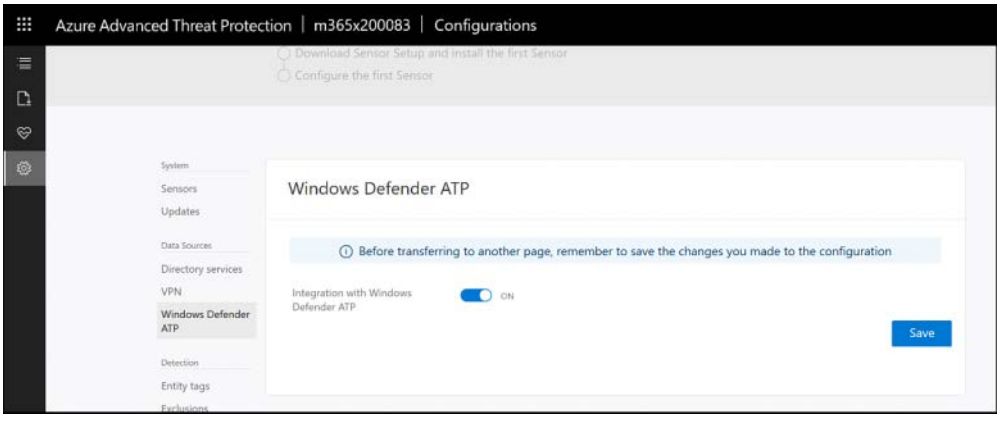

FIGURE 2-4 Integrating Azure ATP with Microsoft Defender ATP (Windows Defender ATP)

Next, access Microsoft Defender ATP at *https://securitycenter.windows.com*, and under **Settings** > **Advanced Features**, enable **Azure ATP Integration** (see Figure 2-5) and click **Save Preferences**.

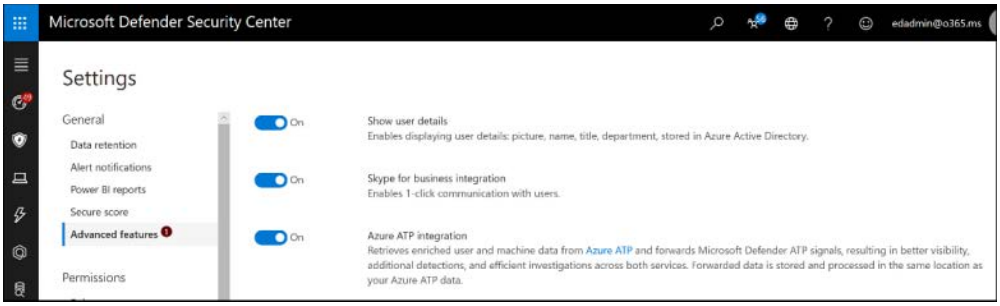

FIGURE 2-5 Integrating Microsoft Defender ATP with Azure ATP

MORE INFO

If you're paying attention, you noticed that Figure 2-4 shows integration between Azure ATP and Microsoft Defender ATP shows "Windows Defender ATP." Microsoft renamed Windows Defender ATP to Microsoft Defender ATP with the introduction of first-party support for Mac OSX and the upcoming support for Linux. It takes time to update all the places it's called Windows Defender ATP, and at the time of this writing, the Azure ATP portal still shows the old name. By the time you're reading this, it will no doubt show the proper name, Microsoft Defender ATP.

Once enabled, if there is a detection in Azure ATP that involves an entity in Microsoft Defender ATP, an icon will appear in the profile for any detection in Azure ATP that will take you to the corresponding information in Microsoft Defender ATP.

Manage suspicious activities

Managing suspicious activities requires that you monitor Azure ATP and review alerts, either in the portal or in the summary emails. When you log in to the Azure ATP portal, you will automatically be taken to the Security Alerts Timeline if there are any Security Alerts. There, you will see alerts in chronological order, starting with the most recent. Alerts will include:

- User, computers, and/or resources involved
- The time of the activity
- Severity
- Status

You can hover your mouse pointer over the alert to surface the mini profile (integration with Microsoft Defender ATP is very valuable here), and you can share the security alert with others through email or download the alert. You can also click the alert to dive deeper into the timeline of the event.

Alerts are categorized as follows, which aligns with the phases in an attack-kill chain:

- Reconnaissance
- Compromised credentials

- Lateral movement
- Domain dominance
- Data exfiltration

By default, preview detections are enabled so that you can see the newest insights. You can disable this in the **Configuration** blade, but it's a good idea to keep these enabled so you are aware of things going on in the environment, even if they are not considered mainstream detections yet.

You can filter security alerts based on **Status**—**All**, **Open**, **Closed**, or **Suppressed**—and by **Severity**; your choices are **High**, **Medium**, and **Low**. You can choose **Suppress Alerts** or **Exclude Entities From Raising Alerts** if you need to reduce the noise from events that, in your specific case, are normal or allowed. For example, you might want to suppress alerts regarding a legacy application that must use LDAP authentication or suppress an administrator who runs a security scanning application against multiple machines. Also, you can delete events.

IMPORTANT

While only Azure ATP Administrators can perform these actions, they really shouldn't perform a delete. Deleting alerts is permanent, and they cannot be restored. Make sure you have long-term storage for alerts; otherwise, you should close alerts instead of deleting them.

Skill 2.2: Implement device threat protection

Endpoints include workstations, servers, laptops, and mobile devices, and they are what your users use to interact with your applications and data every day. Protecting these endpoints is critical to the overall security of your organization, and technologies to help with this include Endpoint Protection, Endpoint Detection and Response, and Threat and Vulnerability Management. In this skill, we will cover Microsoft Defender Advanced Threat Protection and how it is a key component of Microsoft Threat Protection.

IMPORTANT

In early 2019, Microsoft renamed Windows Defender Advanced Threat Protection as Microsoft Defender Advanced Threat Protection; Microsoft made the change largely because it announced that the product would soon include a first-party client for non-Windows platforms. At the time of this writing, the Mac client is generally available, but there are still many Microsoft and other web pages and documentation that use the older name. While Microsoft is working on updating all documentation and consoles to use the new Microsoft Defender ATP name, blog posts and screenshots might still show the older name. Don't let that throw you.

This skill covers how to:

- Plan and implement a Microsoft Defender ATP solution
- Manage Microsoft Defender ATP
- Monitoring Microsoft Defender ATP

Plan and implement a Microsoft Defender ATP solution

Planning and implementing Microsoft Defender ATP is straightforward. You need to be aware of the licensing requirements, the supported operating systems, and the deployment methods available to you. Microsoft Defender ATP is licensed as a part of the Microsoft 365 E5 suite and is also available with Windows Enterprise E5 (and the educational versions of those licenses). Hardware requirements are the same as for the operating systems. Remember, Microsoft Defender ATP is already a part of the Windows 10, Windows Server 2019, and Windows Server 2016 1803 operating systems. Supported operating systems at the time of this writing include:

- Windows 7 SP1 Enterprise
- Windows 7 SP1 Pro
- Windows 8.1 Enterprise
- Windows 8.1 Pro
- Windows 10, version 1607 or later
- Windows Server 2008 R2 SP1
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2016, version 1803
- Windows Server 2019
- macOS Mojave, macOS High Sierra, and macOS Sierra

IMPORTANT

While you can protect servers using Microsoft Defender ATP, the licenses included in Microsoft 365 E5 and Windows E5 only cover the Windows workstation products. To protect servers, you must onboard them to the Azure Security Center, which charges based on a consumption model.

When initially configuring Microsoft Defender ATP, you will choose the location where your data will be stored, which at the time of this writing, includes the United States, the United Kingdom, and the European Union. Once selected, you cannot change this; if you later change your mind, you must tear down and start over again. You will also choose how long data will be stored, with options from 30 to 180 days.

Deployment methods include locally run script, Group Policy Object, SCCM, and Intune, as well as other third-party MDM and software-deployment solutions, as shown in Figure 2-6.

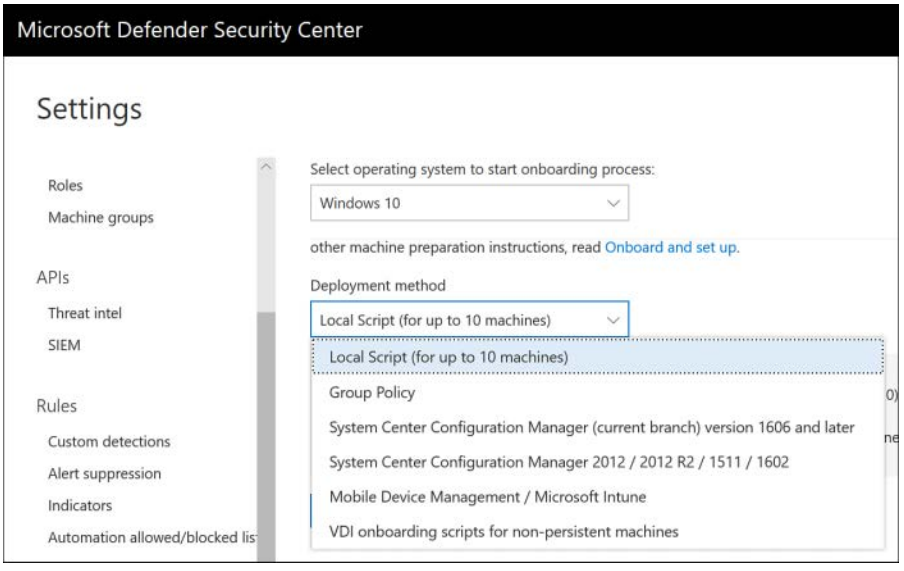

FIGURE 2-6 Microsoft Defender ATP deployment methods

For Windows 10 and Server 2019, deployment is really nothing more than pushing the configuration that specifies the Microsoft Defender ATP tenant and API key used to establish the initial connection. For older operating systems, deployment includes the installation of the Microsoft Defender ATP agent by way of an MSI file. For non-persistent VDI, note that only Windows 10 is supported.

Note that both the Windows diagnostic data service and Windows Defender Antivirus are enabled. If either of these services are disabled, Microsoft Defender ATP onboarding will fail. If you are using a third-party antivirus solution, Windows Defender Antivirus must still be enabled, though it will run in passive mode, and you will want to make sure that the Windows Defender Antivirus Early Launch Antimalware (ELAM) driver is enabled.

Manage Microsoft Defender ATP

Managing Microsoft Defender ATP is as simple as using a supported web browser and being either a Global Administrator or a Security Administrator. Additional RBAC can be configured once Microsoft Defender ATP is initially set up. You can create roles with varied capabilities and assign permissions as appropriate to your organization's needs (see Figure 2-7).

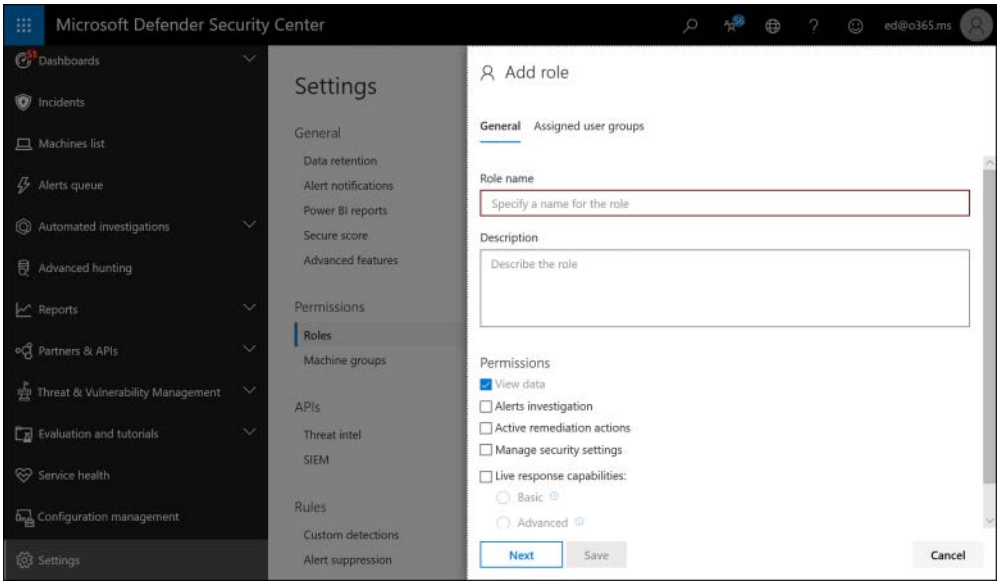

FIGURE 2-7 Adding a role in Microsoft Defender ATP

You should be familiar with each of the areas in the Microsoft Defender ATP console and what you would use each one to do.

Dashboards

Dashboards include information you would want to see first or even to keep on display in a security operations center (SOC). All offer high-level insights, and you can drill down to get more details. The dashboards include Security Operations, Secure Score, and Threat analytics.

Incidents

Anything that Microsoft Defender ATP detects is tracked as an incident. The Incidents area allows you to view and work with incidents. You can filter, classify, and assign incidents and see details. Full details are available in the **Alerts** associated with the incident (see Figure 2-8).

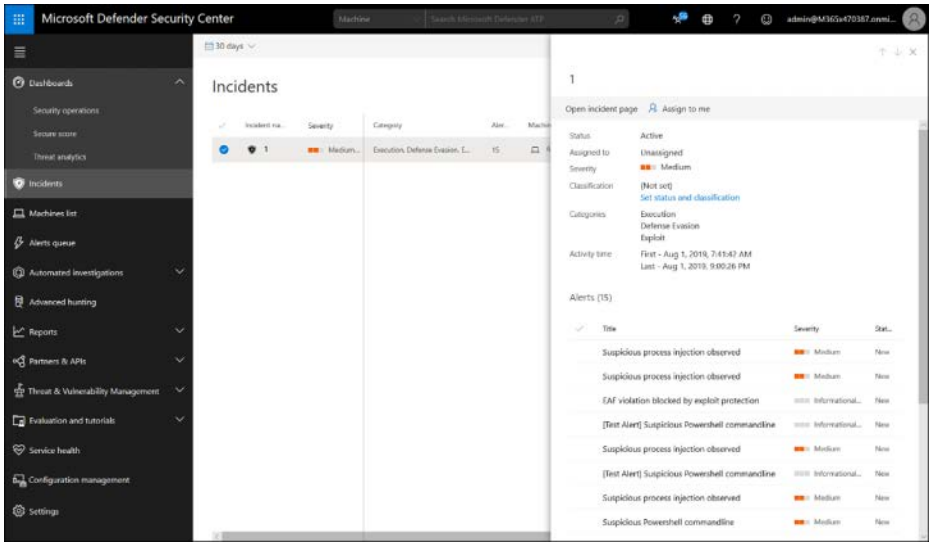

FIGURE 2-8 Incidents in Microsoft Defender ATP

Machines list

The Machines list panel displays all the enrolled machines in Microsoft Defender ATP, enables you to find or filter for a specific machine or version, and allows you to see all details of the machine, including the last logged on user; the IP address of the system; active alerts and incidents; the exposure level; security recommendations; software inventory; and discovered vulnerabilities. You can also choose **Manage Tags**, **Collect Investigation Package**, **Run Anti-Virus Scan**, **Restrict App Execution**, **Isolate Machine**, or **Action Center** (see Figure 2-9).

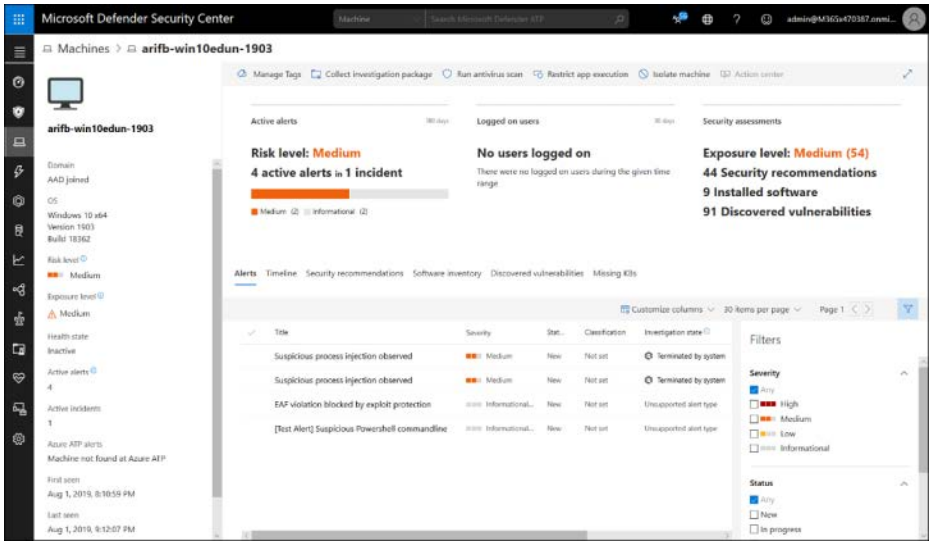

FIGURE 2-9 Viewing a machine from the Machines list

Alerts queue

The Alerts queue shows all alerts in your Microsoft Defender ATP tenant. You can sort and filter to see what alerts are associated to an incident and machine or to a user, and you can boil things down to **Severity**, **Status**, **Investigation State**, **Category**, **Assigned To**, **Detection Source**, **OS Platform**, and/or **Associated Threat**. As with most other things in the console, you can click through to get more details. Once in an alert, you can take actions, including **Manage Alert**, **View Machine Timeline**, **Open Incident Page**, and **Print Alert**, as shown in Figure 2-10.

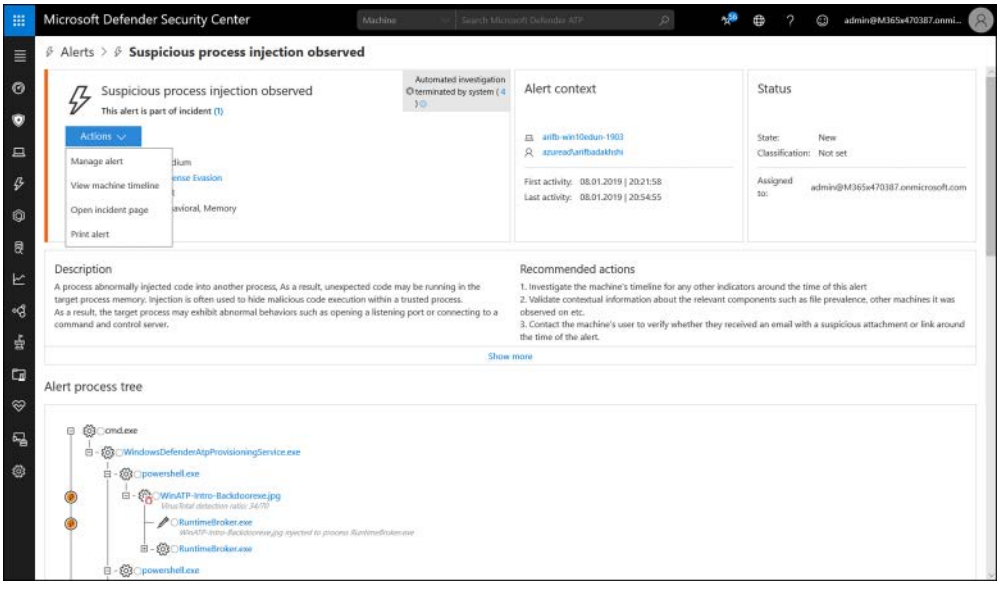

FIGURE 2-10 Viewing an alert in the Alerts queue

Automated Investigations

The Automated Investigations dashboard lists investigations automatically created by the system (see Figure 2-11). By default, it only shows you the past seven days, but you can choose an alternate time or custom date range. It lists all the automated investigations and can be filtered by **Status**, **Triggering Alert**, **Detection Source**, or **Entity**, and each investigation can be clicked to view details including the **Investigation Graph**, **Alerts**, **Machines**, **Key Findings**, **Entities**, **Log**, and **Pending Actions History**.

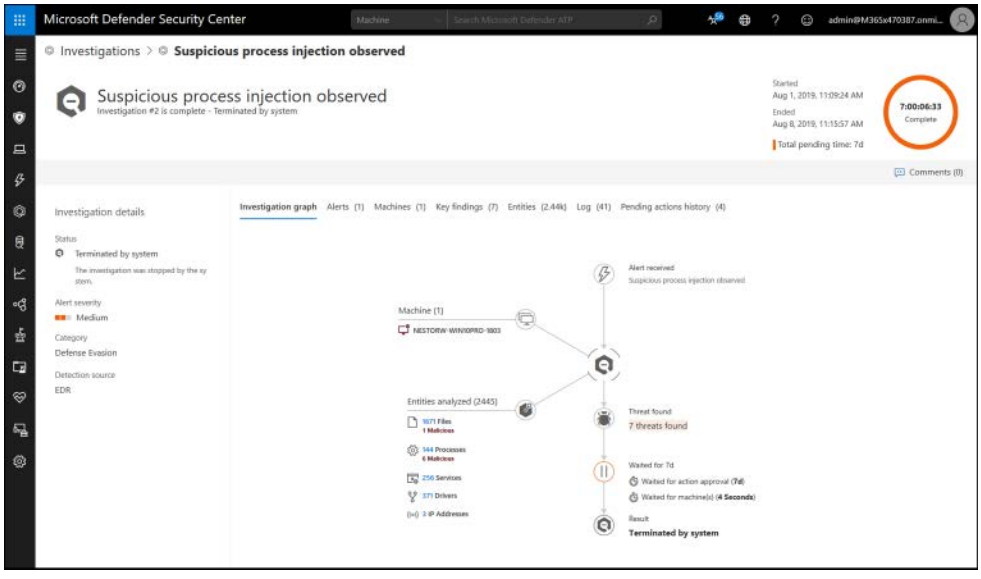

FIGURE 2-11 Viewing an Automated Investigation

Advanced Hunting

The Advanced Hunting dashboard provides an interface to create or paste queries to search data within Microsoft Defender ATP (see Figure 2-12). The Schema provides insight into what can be queried, and the Query Editor lets you create a query from scratch or paste in queries you download from GitHub or other locations. You can save and share queries for future use.

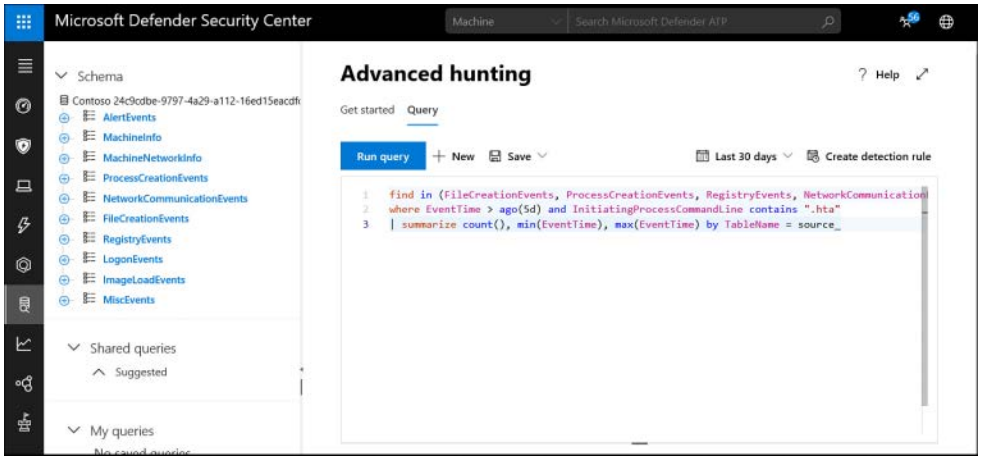

FIGURE 2-12 An Advanced Hunting query using the Kusto Query Language (KQL)

Reports

The Reports dashboard provides graphical summaries of what is going on in your environment and can be filtered like any of the other dashboards. There are two subsections under **Reports**. In the **Threat Protection** section, you can view reports on **Alert Trends** and an **Unsolved Alert Summary** that includes:

- Detection Source
- Category
- Severity
- Status
- Classification And Determination

By default, reports show the past 30 days of information, but you can select other periods or custom date ranges (see Figure 2-13).

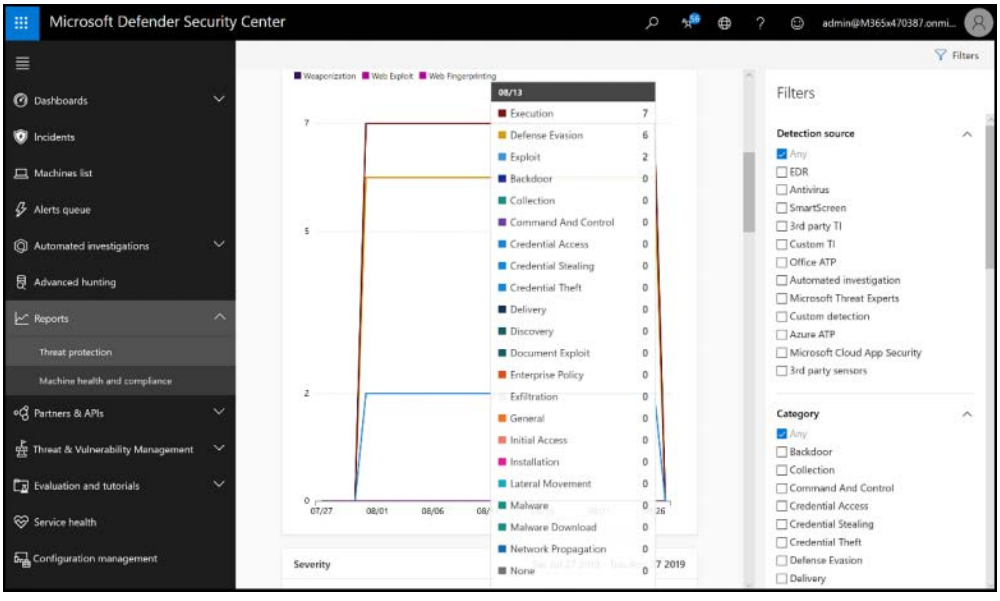

FIGURE 2-13 Viewing Threat Protection reports

In the **Machine Health And Compliance** subsection shown in Figure 2-14, you can view **Machine Trends** and **Machine Summary** for:

- Health State
- Antivirus Status
- OS Platform
- Version

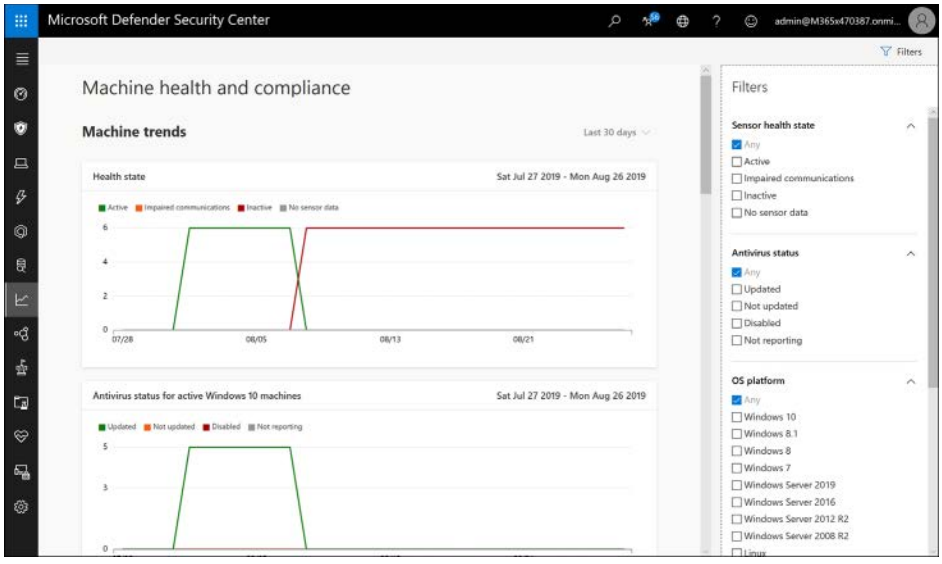

FIGURE 2-14 Viewing Machine Health And Compliance reports

Partners & APIs

The Partners & APIs section includes two sections. The Partner Applications pane displays the many third-party applications that can be integrated with Microsoft Defender ATP. There are several, and more are added frequently. Several can be used to add capabilities for non-Microsoft operating systems, such as Mac or Linux; these include Bitdefender, SentinelOne, and Ziften, as shown in Figure 2-15.

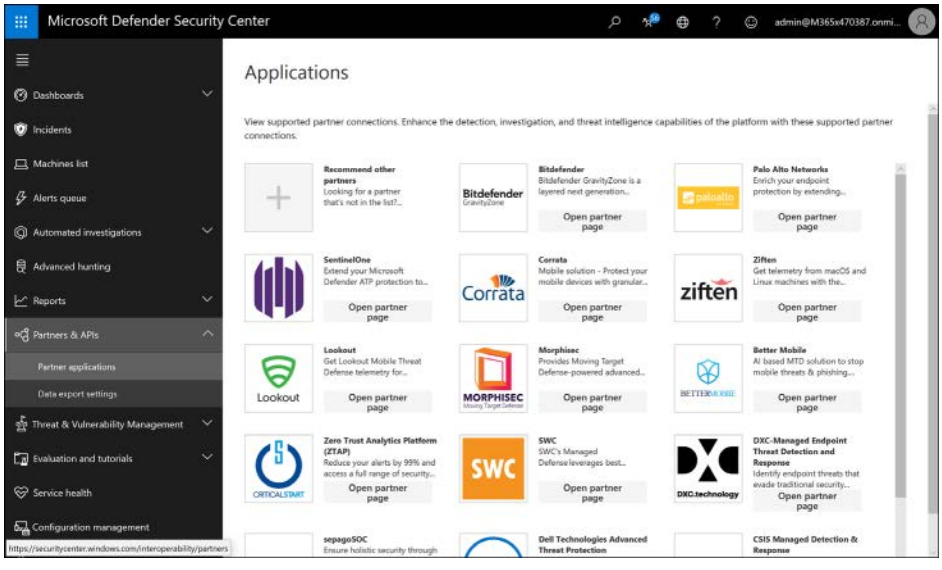

FIGURE 2-15 Viewing Partner Applications in the Partners & APIs dashboard

The Data Export Settings section is where you can choose the data export settings, which are used to push data to other applications, such as SIEMs (see Figure 2-16).

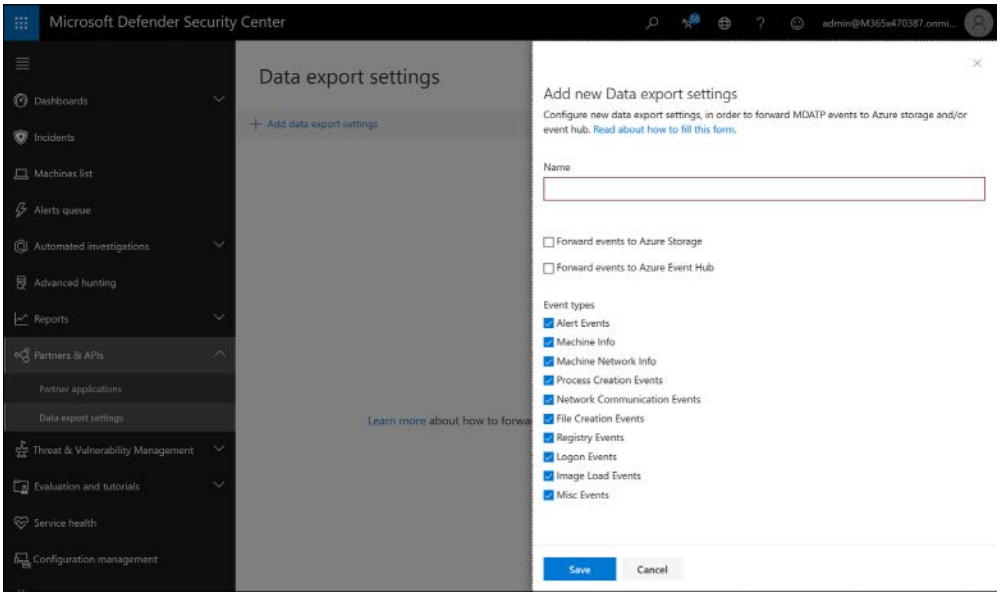

FIGURE 2-16 Add A New Data Export Settings in the Partners & APIs section

Threat & Vulnerability Management Dashboard

The Threat & Vulnerability Management Dashboard (TVM) gives administrators a risk-based, real-time way to discover vulnerabilities in their environments, prioritize them based on risk, and remediate them easily (see Figure 2-17). TVM options are **Dashboard**, **Security Recommendations**, **Remediation**, **Software Inventory**, and **Weaknesses**. The dashboard provides an overview, including the **Exposure Distribution And Configuration Score** to help administrators identify gaps and improve their security postures.

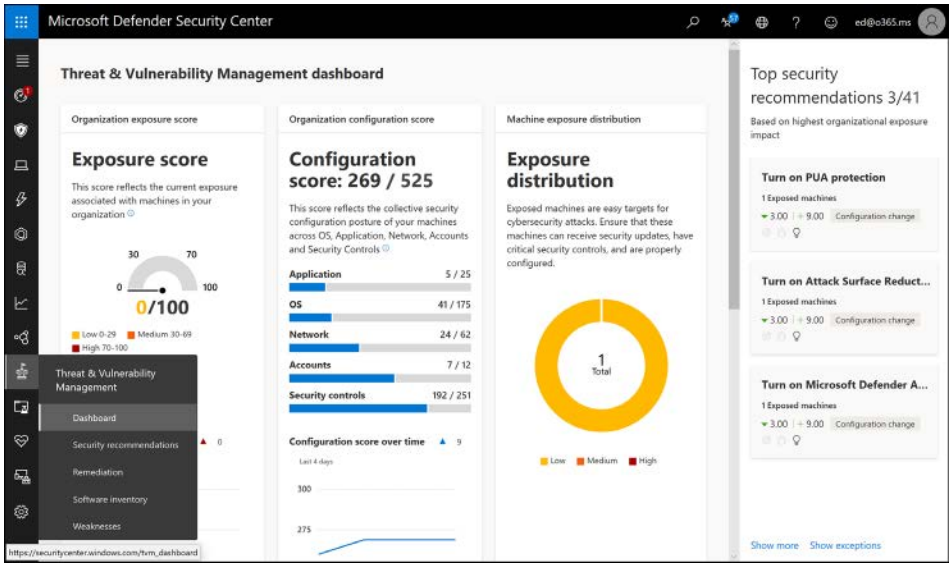

FIGURE 2-17 The Threat & Vulnerability Management Dashboard

Simulations & Tutorials

The Simulations & Tutorials section shown in Figure 2-18 includes the Evaluation Lab and a set of tutorials with simulations so that Microsoft Defender ATP administrators can work in the environment without exposing machines to actual malicious files. The Evaluation Lab lets customers try Microsoft Defender ATP using virtual machines hosted by Microsoft, while the Simulations & Tutorials section can be used against a customer's own machines for testing and learning.

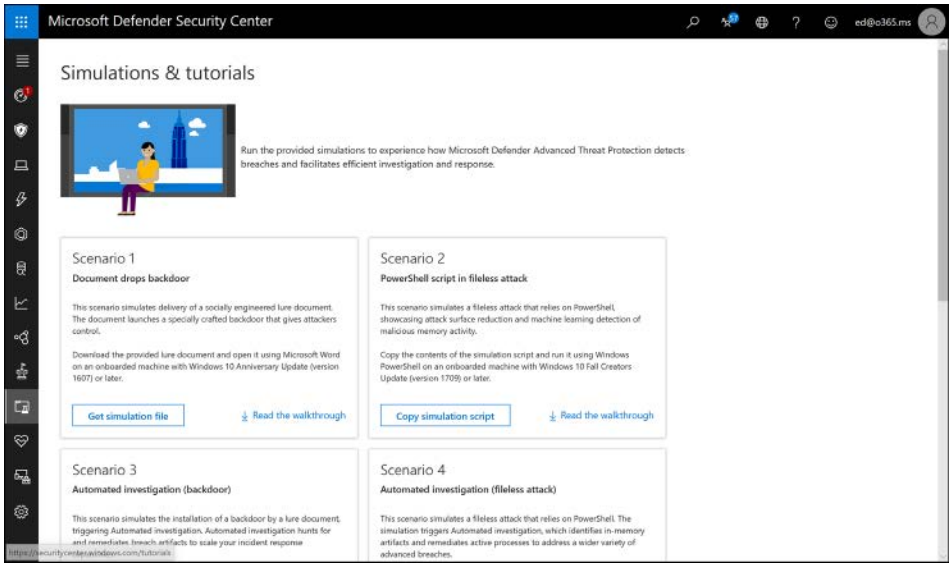

FIGURE 2-18 The Simulations & Tutorials section of Microsoft Defender ATP

Service Health

Service Health is where admins go to check on the overall health of the Microsoft Defender ATP service (see Figure 2-19). If you suspect an issue with the services provided by Microsoft, you can quickly check here to see whether there is an active incident. You can also find historical information on past issues.

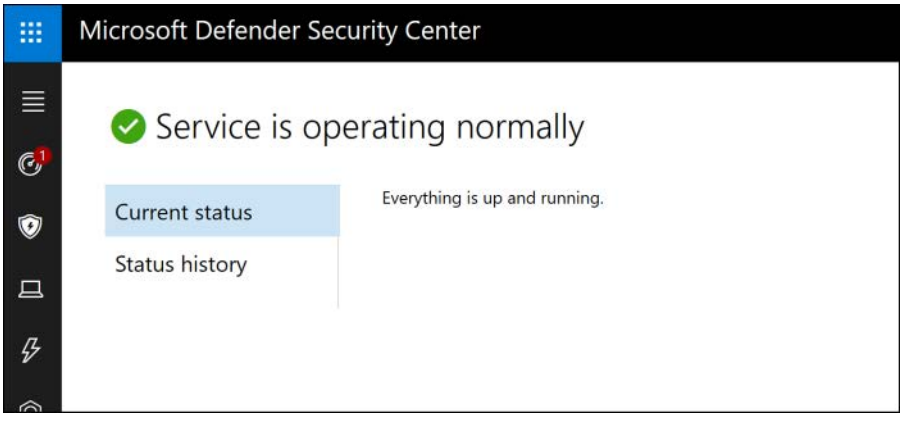

FIGURE 2-19 The Service Health dashboard

Machine Configuration Management

There is a lot included in the Machine Configuration Management dashboard shown in Figure 2-20. You can onboard machines and configure and apply security baselines to enrolled machines through Intune. Also, you can access the appropriate Intune section from here. Additionally, you can jump to the Machine Attack Surface Management section to help enable Windows settings or block possible vectors of attack. These powerful capabilities leverage Intune to apply a standard security posture to all machines.

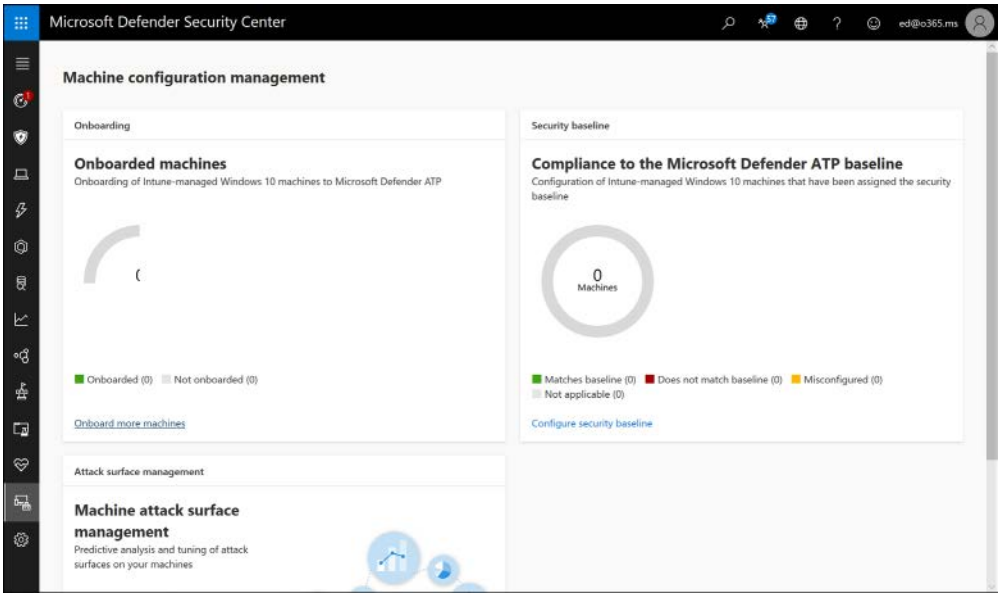

FIGURE 2-20 The Machine Configuration Management dashboard

Settings

The last section is where settings are configured. The settings are broken up into several categories, with options underneath each. They include:

- **General**
  - **Data Retention.** This is where you determine your data is stored (US, UK, or EU) and for how long it is retained (up to 180 days).
  - **Alert Notifications.** This is where you configure email alerts.
  - **Power BI Reports.** This is where you can create PowerBI dashboards.
  - **Secure Score.** This is where you can disable those features you do not want reported on Secure Score because you are addressing the topic with third-party solutions.
  - **Advanced Features.** This is where you enable advanced features, including integration with Office ATP and Azure ATP and enabling previewing features.
- **Permissions**
  - **Roles.** By default, Global Administrators and Security Administrators have full administrative rights in Microsoft Defender ATP, and Security Readers have read-only rights. If you require more granular control, you can enable RBAC and define roles here.
  - **Machine Groups.** If you need to manage different groups of machines in different ways (such as for testing) or if you need to delegate authority to a group you created in RBAC, you can create machine groups and assign permissions to them for management through Microsoft Defender ATP.

- **APIs**
  - **Threat Intel.** This is being replaced with the **Indicators** page under **Rules**.
  - **SIEM.** In this section, you can enable SIEM integration with Azure Sentinel or third-party SIEMs, and you can enable MSSP capabilities to connect to your Microsoft Defender ATP instance.
- **Rules**
  - **Custom Detections.** Custom detection rules are used to identify things that are specific to your environment. They can include Indicators of Compromise (IoCs) that you developed internally, event IDs from custom applications, or any other kind of behavior.
  - **Alert Suppression.** Suppression rules are used to mute alerts that are generated from things you just have to accept in your environment, such as a legacy app that modifies the registry each time it runs.
  - **Indicators.** Here, you can add or import file hashes, IP addresses, URLs, or domains to detect when an enrolled system attempts to access a file or a destination.
  - **Automation Allowed/Blocked Lists.** You can add code-signing certificates here for automatically blocked or allowed files.
  - **Automation Uploads.** In **File Content Analysis**, you can enable or disable the automatic upload of files for analysis within Microsoft Defender ATP, including specific file extensions, and you can enable or disable **Memory Content Analysis**. By default, both are enabled.
  - **Automation Folder Exclusions.** If you have certain proprietary applications that you do not want subject to file content analysis, you can exempt their file paths here without disabling the protection for everything else.
- **Machine Management**
  - **Onboarding.** As discussed previously, this is where you download onboarding scripts or the installers for downstream clients.
  - **Offboarding.** As discussed previously, this is where you download offboarding scripts. Make sure you note that offboarding scripts must be refreshed every 30 days and that their file name includes the "use by" date.

EXAM TIP

You should be familiar with what you can do in each of the sections of the Microsoft Defender ATP UI. If you have used Microsoft Defender ATP in production, this should be easy. However, if you are not actively using Microsoft Defender ATP, take the time to be sure you can list what is done where.

Monitoring Microsoft Defender ATP

Monitoring Microsoft Defender ATP is straightforward. If your team is actively managing endpoints, then they will likely be logged into Microsoft Defender ATP and using the console throughout their work. The Security operations dashboard is designed to surface the most useful information, making it easy to determine at a glance if any actions are required. You can see the service health, at-risk machines and users, see active alerts, and determine if any machines are having sensor issues or are not reporting to the service.

You can also integrate Microsoft Defender ATP with your SIEM. Microsoft's own SIEM—Azure Sentinel—is supported, as are both Splunk and HP ArcSight. Other SIEMs can connect using a generic connector or by using a REST API.

Skill 2.3: Implement and manage device and application protection

This objective focuses on several of the built-in protections within Microsoft Windows 10 Enterprise Edition, as well as additional protections that can be applied to applications and to data. We will first look at Windows 10 features and then move on to additional protections.

This skill covers how to:

- Plan for device protection
- Configure and manage Windows Defender Application Guard
- Configure and manage Windows Defender Application Control
- Configure and manage Windows Defender Exploit Guard
- Configure Secure Boot
- Configure and manage Windows 10 device encryption
- Plan for securing applications data on devices
- Define managed apps for mobile application management (MAM)
- Protect your enterprise data using Windows Information Protection (WIP)
- Configure WIP policies
- Configure Intune App Protection Policies for non-Windows devices

Plan for device protection

Windows 10 includes several features to help protect devices from malicious activity. These features can be managed by the user, they can be centrally managed using Group Policy for domain-joined systems, or they can be managed using Intune for Azure AD–joined systems. You can access the features directly by pressing the Start button, typing **device security**, and pressing **Enter**. See the Device Security dashboard in Figure 2-21.

Index

A

B

C

D

E

F

G

H

I

J–K–L

M

N

O

P

Q

R

S

T

U

V

W

X–Y–Z