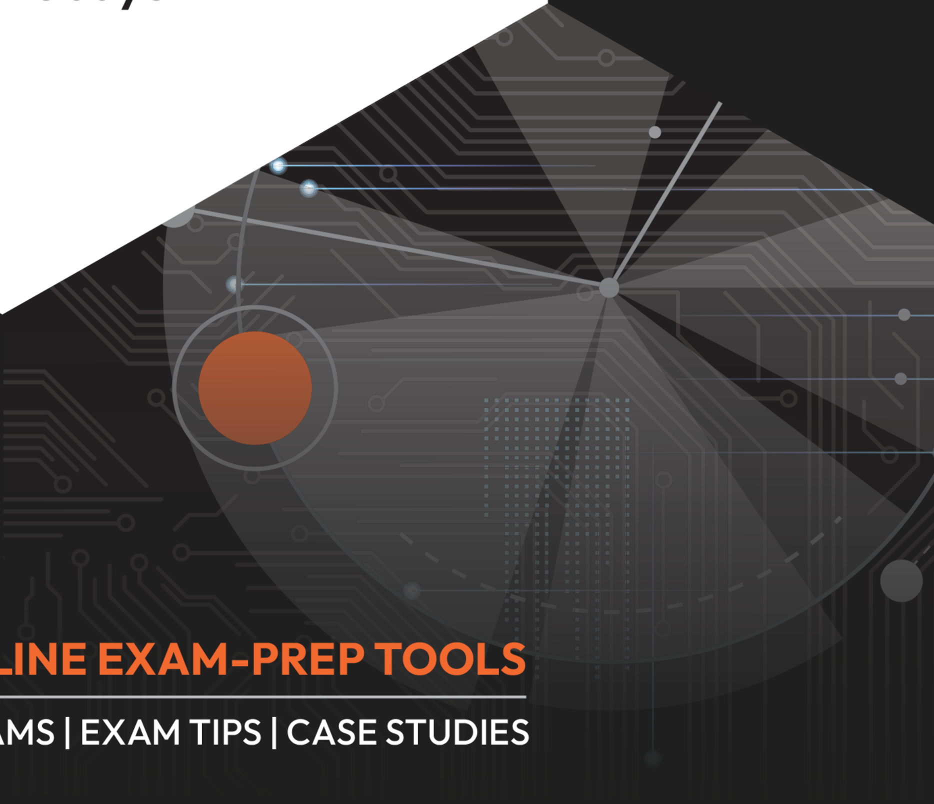
‹packt›

Second Edition

Microsoft Cybersecurity Architect Exam Ref SC-100

Ace the SC-100 exam and develop cutting-edge cybersecurity strategies

Dwayne Natwick
Graham Gold | Abu Zobayer



INCLUDES FREE ONLINE EXAM-PREP TOOLS

FLASHCARDS | MOCK EXAMS | EXAM TIPS | CASE STUDIES

Microsoft Cybersecurity Architect Exam Ref SC-100

Second Edition

Ace the SC-100 exam and develop cutting-edge cybersecurity strategies

Dwayne Natwick

Graham Gold

Abu Zobayer

packt

Microsoft Cybersecurity Architect Exam Ref SC-100

Second Edition

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the authors, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Authors: Dwayne Natwick, Graham Gold, and Abu Zobayer

Reviewers: Dan Gora and Jetro Wils

Publishing Product Manager: Anindya Sil

Development Editor: Richa Chauhan

Digital Editor: M Keerthi Nair

Presentation Designer: Shantanu Zagade

Editorial Board: Vijin Boricha, Megan Carlisle, Simon Cox, Ketan Giri, Saurabh Kadave,
Alex Mazonowicz, Gandhali Raut, and Ankita Thakur

First Published: January 2023

Second Edition: October 2024

Production Reference: 1311024

Published by Packt Publishing Ltd.
Grosvenor House
11 St Paul's Square
Birmingham
B3 1RB

ISBN: 978-1-83620-851-8

`www.packtpub.com`

Contributors

About the Authors

Dwayne Natwick is the **CEO/Owner/Principal Trainer** at Captain Hyperscaler, LLC. He was previously the Global Principal Cloud Security Lead at Atos, a multi-cloud GSI. He has been in IT, security design, and architecture for over 30 years. His love of teaching led him to become an APMG-accredited ISACA trainer, a **Microsoft Certified Trainer** (**MCT**) Regional Lead and a **Microsoft Most Valuable Professional** (**MVP**), an AKYLADE Certified Instructor, and an ISC2 Authorized Instructor.

Dwayne has a master's degree in business IT from Walsh College; the CISM, CISA, and CRISC certifications from ISACA; the CISSP, CGRC, CSSLP, CCSP, SSCP, and CC certifications from ISC2; and over 18 Microsoft certifications, including Identity and Access Administrator, Azure Security Engineer, and Microsoft 365 Security Administrator. Dwayne can be found sharing information via social media, industry conferences, his blog site, and his YouTube channel.

Originally from Maryland, Dwayne currently resides in Michigan with his wife and three children.

To my wife, Kristy, thank you for always being there and supporting me. You are the love of my life and my best friend. To my children, Austin, Jenna, and Aidan, even with my career accomplishments, you are what makes me the proudest. You are all growing up to be such amazing people with kind hearts.

All four of you are my world and I could not make this journey without you.
All my love and support for everything that you do.

– Dwayne Natwick

Graham Gold is a Senior Cloud Security Engineer at Admiral Group. He has 27 years' experience in financial services IT, now specializing in cloud security as of 2020. He has been instrumental in designing, building, securing, and running complex systems at enterprise scale across mainframes, Windows, Linux, and networks, on both on-premises systems and cloud platforms.

He is a multi-cloud certified professional, holding the Microsoft Cybersecurity Architect Expert, Azure Security Engineer, Google Certified Professional Cloud Security Engineer, and Google Certified Professional Cloud Architect certifications.

Graham is passionate about identity security and privileged access management, and loves to help his colleagues and community, sharing his knowledge on his blog and across social media platforms. Outside of work, he lives in Scotland with his wife and cats, and they share a love of world travel.

Abu Zobayer works as a Senior Cloud Solutions Architect at Microsoft, bringing over two decades of experience in the IT industry. Over the course of his career, he has taken on various key roles, such as Principal Microsoft Technical Trainer and Senior Customer Engineer. His credentials include a range of certifications: Microsoft Cybersecurity Architect Expert, Azure Security Engineer, Azure DevOps Expert, and Azure Solutions Architect Expert.

Abu holds a master's degree in cybersecurity from the University of Texas. He has played a crucial role in designing, deploying, and securing advanced cloud architectures, ensuring reliable and scalable solutions for enterprise-level clients.

Abu has a strong interest in cybersecurity and cloud innovations, and he frequently shares his expertise through training programs and community initiatives. Outside of his professional life, he enjoys experimenting with new technologies and spending quality time with his family in San Antonio, Texas.

About the Reviewers

Dan Gora is a Lead Cloud Security Architect at Eviden, part of ATOS, with over 15 years of experience in cybersecurity. Specializing in secure cloud transformation for highly regulated industries, he has guided organizations to enhance their security architecture by effectively implementing DevSecOps and zero-trust methodologies.

As an active contributor to the cybersecurity community, Dan is the OWASP Frankfurt Chapter Lead and Board Member of OWASP Germany. He has also co-authored several whitepapers for the Cloud Security Alliance. Dan holds a master's degree in secure software engineering from Darmstadt University of Applied Sciences, Germany, and certifications such as CISSP, CSSLP from ISC2, and CCSK from CSA, along with multiple credentials from Microsoft and AWS.

Originally from Germany, Dan now lives in Scotland with his civil partner, Margaretha.

To my partner, Margaretha, thank you for your unwavering love and support throughout the years. You are the cornerstone of my life and instrumental to my success. I cherish every moment with you.

– Dan Gora

Jetro Wils helps organizations operate safely in this cloud era by strengthening their information security and compliance, thus reducing risk and providing peace of mind. For 18 years, Jetro has been active in various tech companies in Belgium. Jetro's focus is practical cybersecurity advisory, specializing in cloud security, governance, compliance, and risk management. Jetro is a three-time Microsoft Certified Azure Expert and an MCT. He gives 10-20 certified training sessions annually on the cloud, AI, and security and has trained over 100 professionals, including enterprise architects, project managers, service managers, salespeople, team leaders, and engineers. He also hosts the BlueDragon Podcast, focusing on the above topics for decision-makers. Jetro is currently pursuing a master's degree in IT risk and cybersecurity management at the Antwerp Management School. He is a certified NIS 2 Lead Implementor, having gained the certification from PECB.

Table of Contents

4

Design an Identity Security Strategy 87

5

Design a Regulatory Compliance Strategy 115

6

Evaluate Security Posture and Recommend Technical Strategies to Manage Risk 133

7

Design a Strategy for Securing Server and Client Endpoints 165

8

Design a Strategy for Securing SaaS, PaaS, and IaaS 191

9

Specify Security Requirements for Applications 221

10

11

Preface

As the adoption of cloud infrastructure and services continues to grow at a rapid pace, cloud security has never been more critical. Businesses are increasingly moving their data, services, and applications to the cloud, creating a need for skilled professionals who can secure these environments. Cloud computing has evolved from a supplementary technology to a core competency within enterprises.

This shift has created a high demand for knowledgeable cloud security engineers and architects who can design, build, and operate secure cloud environments. The challenges posed by numerous security threats require organizations to develop robust cloud security strategies. Certifications play a vital role in identifying and developing the necessary skills for implementing cloud security measures. They also help individuals demonstrate their expertise to potential employers, advancing their careers.

The goal of this book is to equip you with the knowledge and skills needed to excel in cloud security. It covers a comprehensive range of topics essential for understanding and implementing cloud security measures. From cybersecurity fundamentals to advanced topics such as incident response, this book provides practical and straightforward explanations designed to educate you on the challenges and solutions in cloud security.

This book will prepare cybersecurity professionals like you for the SC-100 exam while also giving you a solid foundation that will help you put your knowledge to work and implement the strategies you learn. A mixture of theoretical and practical knowledge, practice questions, and a mock exam will ensure you breeze through the exam.

As you progress through this book, you will engage with various cloud security concepts and practices. The chapters cover critical areas such as cybersecurity in the cloud, building a security strategy, identity and access management, data protection, compliance, incident response, security operations, and future trends. Each chapter is designed to guide you through scenarios that test your understanding and application of cloud security principles.

By the end of this book, you will have a solid understanding of cloud security principles and practices and the confidence to apply this knowledge in your current role. You will be well prepared to tackle the challenges of securing cloud environments and stay ahead of emerging threats and technologies.

Who This Book Is For

This book is for a wide variety of cybersecurity professionals – from security engineers and cybersecurity architects to Microsoft 365 administrators, user and identity administrators, infrastructure administrators, cloud security engineers, and other IT professionals preparing to take the SC-100 exam. It is also a good resource for those who are designing cybersecurity architecture but not preparing for the exam. To get started, you will need a solid understanding of the fundamental services within Microsoft 365 and Azure, along with the security, compliance, and identity capabilities of Microsoft and hybrid architectures.

What This Book Covers

Chapter 1, Cybersecurity in the Cloud, provides an overview of cybersecurity and its evolution with cloud technologies. It explains how cybersecurity has changed as workloads have moved from on-premises data centers to the cloud.

Chapter 2, Build an Overall Security Strategy and Architecture, discusses developing and designing a security strategy for cloud, hybrid, and multi-tenant environments. It includes identifying integration points, translating business goals into security requirements, and designing security for resiliency.

Chapter 3, Design a Security Operations Strategy, covers designing and evaluating a strategy for security operations. Topics include logging and auditing for public, hybrid, and multi-cloud infrastructures, utilizing SIEM and SOAR solutions, and managing the incident life cycle.

Chapter 4, Design an Identity Security Strategy, focuses on creating an identity security strategy for cloud-native, hybrid, and multi-cloud environments. It emphasizes zero-trust principles and covers strategies for access management, conditional access, and privileged role access.

Chapter 5, Design a Regulatory Compliance Strategy, explores developing security and governance strategies based on regulatory compliance requirements. It includes using tools such as Microsoft Defender for Cloud and Azure Policy to evaluate and govern resources.

Chapter 6, Evaluate Security Posture and Recommend Technical Strategies to Manage Risk, discusses assessing security posture using benchmarks and tools such as Microsoft Defender for Cloud. It covers recommending security capabilities to mitigate identified risks.

Chapter 7, Design a Strategy for Securing Server and Client Endpoints, details creating security baselines and specifying security requirements for servers, mobile devices, and AD DS. It also covers managing secrets, keys, and certificates, and securing remote access.

Chapter 8, Design a Strategy for Securing SaaS, PaaS, and IaaS, involves building security baselines and specifying security requirements for various cloud services and workloads, including containers, edge computing, and application services.

Chapter 9, Specify Security Requirements for Applications, establishes security standards and strategies for applications and APIs. It includes prioritizing threat mitigation, onboarding new applications, and designing security solutions for API management.

Chapter 10, Design a Strategy for Securing Data, applies risk management frameworks and encryption standards to protect sensitive data. It covers identifying and protecting sensitive data and specifying encryption standards for data at rest and in motion.

How to Get the Most Out of This Book

This book is crafted to equip you with the knowledge and skills necessary to excel in the SC-100 exam through memorable explanations of major domain topics. It covers the core domains critical to cloud security and cybersecurity expertise that candidates must be proficient in to pass the exam. For each domain, you will work through content that reflects real-world cloud security challenges. At certain points in the book, you will assess your understanding by taking chapter-specific quizzes. This not only prepares you for the SC-100 exam but also allows you to dive deeper into a topic as needed based on your results.

Online Practice Resources

With this book, you will unlock unlimited access to our online exam-prep platform (*Figure 0.1*). This is your place to practice everything you learn in the book.

> **How to Access These Materials**
>
> To learn how to access the online resources, refer to *Chapter 11*, *Accessing the Online Practice Resources*, at the end of this book.

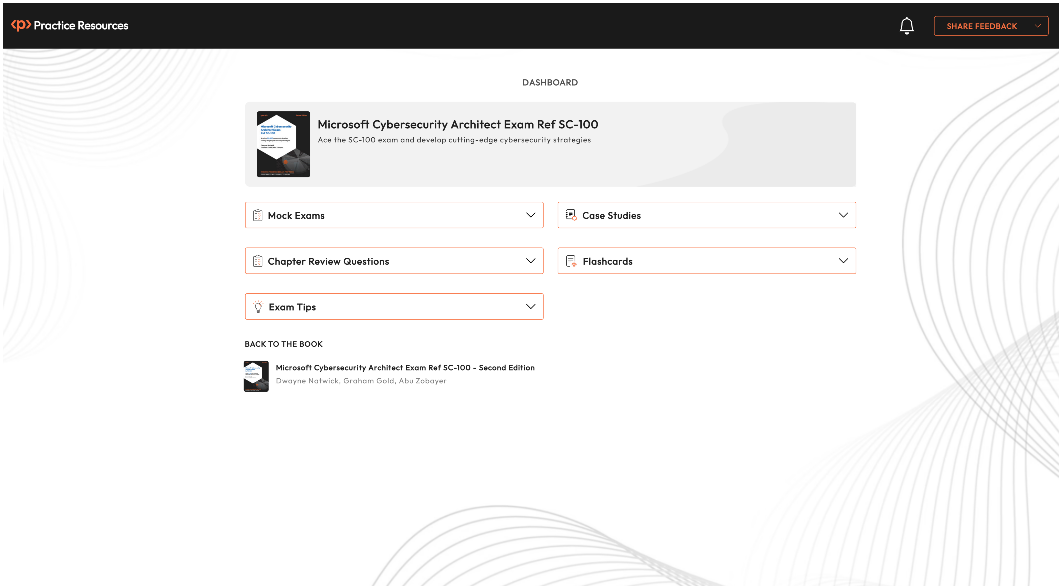

Practice Resources
SHARE FEEDBACK
DASHBOARD
Microsoft Cybersecurity Architect Exam Ref SC-100
Ace the SC-100 exam and develop cutting-edge cybersecurity strategies
Mock Exams
Case Studies
Chapter Review Questions
Flashcards
Exam Tips
BACK TO THE BOOK
Microsoft Cybersecurity Architect Exam Ref SC-100 - Second Edition
Dwayne Natwick, Graham Gold, Abu Zobayer

Figure 0.1: Online exam-prep platform on a desktop device

Sharpen your knowledge of SC-100 exam concepts with multiple sets of mock exams, interactive flashcards, case studies, and exam tips accessible from all modern web browsers.

Download the Color Images

We also provide a PDF file that has color images of the screenshots/diagrams used in this book. You can download it here: `https://packt.link/SC-100_GraphicBundle`.

Conventions Used

There are several text conventions used throughout this book.

`Code in text`: Indicates code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and X (formerly Twitter) handles. Here is an example: "`Since '1'='1'` is always true, this query will always return all data from the `users` table, giving the malicious user access to all user accounts."

A block of code is set as follows:

```
SELECT * FROM users WHERE username = 'username' AND password =
'password'
```

Bold: Indicates a new term, an important word, or words that you see onscreen. For example, words in menus or dialog boxes appear in the text like this. Here is an example: "**Infrastructure as a Service** (**IaaS**) offers virtualized computing resources, including **Virtual Machines** (**VMs**), storage, and networking. The user controls their infrastructure, while the **Cloud Service Provider** (**CSP**) oversees the physical hardware.

Tips or Important Notes

Appear like this.

Get in Touch

Feedback from our readers is always welcome.

General feedback: If you have any questions about this book, please mention the book title in the subject of your message and email us at `customercare@packt.com`.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you could report this to us. Please visit `www.packtpub.com/support/errata` and complete the form. We ensure that all valid errata are promptly updated in the GitHub repository at `https://packt.link/SC100e2GitHub`.

Piracy: If you come across any illegal copies of our works in any form on the internet, we would be grateful if you could provide us with the location address or website name. Please contact us at `copyright@packt.com` with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit `authors.packtpub.com`.

Share Your Thoughts

Once you've read *Microsoft Cybersecurity Architect Exam Ref SC-100, Second Edition*, we'd love to hear your thoughts! Please `click here to go straight to the Amazon review page` for this book and share your feedback.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Download a Free PDF Copy of This Book

Thanks for purchasing this book!

Do you like to read on the go but are unable to carry your print books everywhere?

Is your eBook purchase not compatible with the device of your choice?

Don't worry – now, with every Packt book, you get a DRM-free PDF version of that book at no cost.

Read anywhere, any place, on any device. Search, copy, and paste code from your favorite technical books directly into your application.

The perks don't stop there: you can get exclusive access to discounts, newsletters, and great free content in your inbox daily.

Follow these simple steps to get the benefits:

1. Scan the QR code or visit the link below it:

   `https://packt.link/free-ebook/9781836208518`

2. Submit your proof of purchase.
3. That's it! We'll send your free PDF and other benefits to your inbox directly.

1

Cybersecurity in the Cloud

This chapter will provide an overview of what cybersecurity is and why it matters in modern business.

It is important to look beyond news headlines and understand the business context, business challenges, threat scenarios, and impacts. Beyond passing the exam, the aim of this book is to enable you, as a cybersecurity practitioner, to protect your business while ensuring it can take advantage of business growth opportunities safely.

Often, you will discover that the choices that you need to make to balance these objectives are not binary choices; you need the business and threat context to make the correct decisions for your business. This chapter will also discuss the evolution of cybersecurity and cyber-attacks as cloud technologies have become more prevalent. Once you have completed this chapter, you will understand what cybersecurity means and how it has changed as we have moved our workloads from on-premises data centers to the cloud.

Overall, this chapter covers key exam domains and topics, specifically **Designing solutions that align with security best practices and priorities (20–25%)**. This includes creating a security strategy to support business resiliency, identifying and prioritizing threats to critical assets, and developing solutions for **business continuity and disaster recovery** (**BCDR**) in hybrid and multi-cloud environments, as well as mitigating ransomware attacks with a focus on BCDR and privileged access.

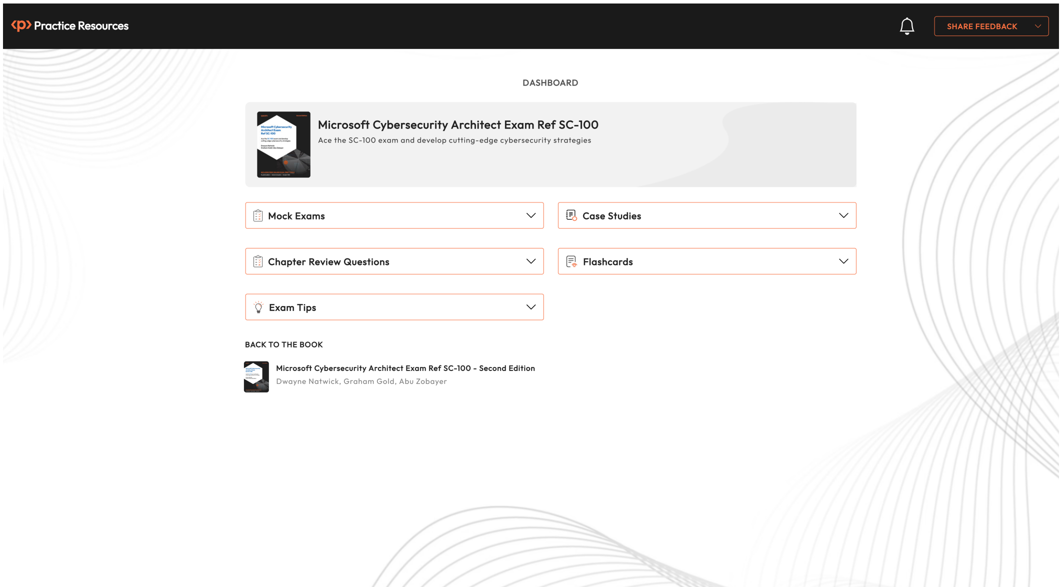
Making the Most of This Book – Your Certification and Beyond

This book and its accompanying online resources are designed to be a complete preparation tool for your **SC-100 exam**.

The book is written in a way that means you can apply everything you've learned here even after your certification. The online practice resources that come with this book (*Figure 1.1*) are designed to improve your test-taking skills. They are loaded with timed mock exams, chapter review questions, interactive flashcards, case studies, and exam tips to help you work on your exam readiness from now till your test day.

Before You Proceed

To learn how to access these resources, head over to *Chapter 11*, *Accessing the Online Practice Resources*, at the end of the book.



Microsoft Cybersecurity Architect Exam Ref SC-100

Ace the SC-100 exam and develop cutting-edge cybersecurity strategies

Microsoft Cybersecurity Architect Exam Ref SC-100 - Second Edition

Dwayne Natwick, Graham Gold, Abu Zobayer

Figure 1.1: Dashboard interface of the online practice resources

Here are some tips on how to make the most of this book so that you can clear your certification and retain your knowledge beyond your exam:

1. Read each section thoroughly.
2. **Make ample notes**: You can use your favorite online note-taking tool or use a physical notebook. The free online resources also give you access to an online version of this book. Click the `BACK TO THE BOOK` link from the dashboard to access the book in **Packt Reader**. You can highlight specific sections of the book there.
3. **Chapter review questions**: At the end of this chapter, you'll find a link to review questions for this chapter. These are designed to test your knowledge of the chapter. Aim to score at least **75%** before moving on to the next chapter. You'll find detailed instructions on how to make the most of these questions at the end of this chapter in the *Exam Readiness Drill – Chapter Review Questions* section. That way, you're improving your exam-taking skills after each chapter, rather than at the end of the book.
4. **Flashcards**: After you've gone through the book and scored **75%** or more in each of the chapter review questions, start reviewing the online flashcards. They will help you memorize key concepts.
5. **Mock exams**: Revise by solving the mock exams that come with the book till your exam day. If you get some answers wrong, go back to the book and revisit the concepts you're weak in.
6. **Exam tips**: Review these from time to time to improve your exam readiness even further.

In this chapter, we are going to cover the following main topics:

- What is cybersecurity?
- The evolution of cybersecurity from on-premises to the cloud
- Cybersecurity architecture use cases
- Understanding the scope of cybersecurity in the cloud

What Is Cybersecurity?

To be able to understand the role of the **cybersecurity architect**, you should first understand what is meant by the term cybersecurity. The term is used in many different contexts within security, compliance, and identity.

Cybersecurity refers to the practice of protecting systems, networks, and programs from digital attacks. These cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money from users, or interrupting normal business processes.

Significance in Modern Business

In today's digital age, cybersecurity is crucial for several reasons:

- **Protection of data**: Businesses handle vast amounts of sensitive data, including personal information, financial records, and intellectual property. Cybersecurity measures help protect this data from breaches and theft.
- **Business continuity**: Cyber-attacks can disrupt business operations, leading to significant downtime and financial losses. Effective cybersecurity ensures that businesses can continue to operate smoothly.
- **Reputation management**: A data breach can severely damage a company's reputation. Strong cybersecurity practices help maintain customer trust and protect the brand's image.
- **Compliance**: Many industries are subject to regulations that require robust cybersecurity measures. Compliance with these regulations is essential to avoid legal penalties and maintain operational integrity.

Cybersecurity in the Context of the SC-100 Exam

The SC-100: Microsoft Cybersecurity Architect exam is designed for professionals who translate cybersecurity strategies into actionable capabilities that protect an organization's assets, business, and operations. Key areas covered in the exam include the following:

- **Zero-trust principles**: Implementing security strategies that assume breaches will occur and verifying each request as though it originates from an open network.
- **Identity and access management**: Ensuring that only authorized users have access to specific resources.
- **Platform protection**: Safeguarding the underlying infrastructure, including servers and networks.
- **Security operations**: Monitoring and responding to security incidents.
- **Data and AI security**: Protecting data and AI models from unauthorized access and manipulation.
- **Application security**: Ensuring that applications are secure from development through deployment.
- **Governance and risk compliance (GRC)**: Designing solutions that meet regulatory requirements and manage risk effectively.

Preparing for the SC-100 exam involves understanding these concepts and being able to design and implement security solutions that align with best practices and organizational needs.

To set a base level of understanding for this book, we will use the definitions provided by **NIST**, the **National Institute of Standards and Technology**. The reason for doing this is that many organizations use procedures and guidance from NIST and other agencies as the foundations of their own security standards, controls, and procedures.

According to NIST, there are multiple definitions for the term cybersecurity; the first part of the NIST definition is *"the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentications, confidentiality, and nonrepudiation."*

Cybersecurity is also defined by NIST as *"the prevention of damage to, unauthorized use of, exploitation of, and – if needed – the restoration of electronic information and communications systems and the information they contain, in order to strengthen the confidentiality, integrity, and availability of these systems."*

Taken together, this can be stated more simply: cybersecurity is the defense of electronic communications, systems, and information, ensuring that they remain available, accurate, and consistent, and confidential information remains so.

Notice also that there is emphasis placed on the ability to recover communications, systems, and information from any event, whether malicious or not.

Finally, notice that nonrepudiation is explicitly mentioned. It is not enough to be able to recover from an event; you must also be able to attribute every action or event to the true source of that event due to legal and regulatory obligations that most businesses will have to adhere to depending on their legal and geographic jurisdiction.

Overall, the underlying factors here are that you must take the steps to provide assurance for maintaining the confidentiality, integrity, and availability of your data and systems.

Note

The glossary at the following URL links to a plethora of NIST publications that give detailed cybersecurity guidance and, as such, is a notable example of how cybersecurity might be implemented in organizations that you work for now and in the future. It is advisable to read these documents. Though it is not required for the exam, they will be advantageous to you in your career in cybersecurity: `https://csrc.nist.gov/glossary/term/cybersecurity`.

In the next section, you will learn more about how the role of cybersecurity has changed from an on-premises to a cloud network and infrastructure.

Evolution of Cybersecurity from On-Premises to the Cloud

When protecting an **on-premises** data center and infrastructure, a cybersecurity architect designs various controls to safeguard physical assets and prevent unauthorized access at physical data center entry points or **internet service provider** (**ISP**) network entry points. Traditionally, these protections included a combination of physical security appliances, such as firewalls for packet inspection, and endpoint protection by allowing access to the data center only through SSL VPN-encrypted connections. These devices were managed by the company and given antivirus and anti-malware software to mitigate potential attacks.

As companies transition to more cloud-native applications, such as Microsoft 365, and build infrastructure on cloud providers like Microsoft Azure, the responsibility for security shifts from physical to virtual environments. This creates new vulnerabilities that the company must identify and plan ways in which to mitigate against threats. The following sections will discuss how a cybersecurity architect should plan for protection and controls within cloud and hybrid infrastructures.

Defense-in-Depth Security Strategy

When protecting cloud and hybrid infrastructure, there are many aspects that need to be considered. As you go through the various solutions offered within **Microsoft 365** and **Azure**, such as Microsoft Sentinel, the Microsoft Defender suite, and Microsoft Entra, the defense-in-depth methodologies and principles, which are explained in the next section, are essential for effectively protecting resources, identity, and data.

Building a Defense-in-Depth Security Posture

To protect your company from cyber-attacks, it is essential to implement controls that address each stage of an attack and maintain a defense-in-depth security posture. This approach ensures multiple layers of protection, making it harder for attackers to penetrate your defenses.

When considering your infrastructure, there are many logical layers that could potentially be breached through misconfiguration or exploitation of vulnerabilities.

These layers are shown in *Figure 1.2*.

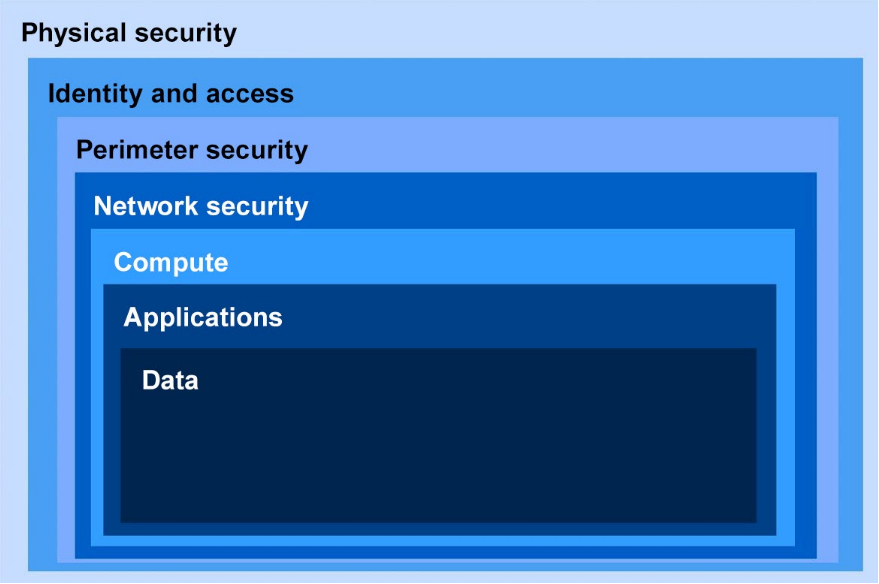


Figure 1.2: Logical layers of defense-in-depth posture/infrastructure

In *Figure 1.2*, we see the logical layers in the technology stack. It is these layers where an attacker may be able to gain access to systems and/or data.

In the following sections, you will explore these logical layers in depth, learning what each layer entails and how they can be secured.

Physical Layer

The **Physical** layer of defense includes the actual hardware technology and spans the entire data center facility. This includes the compute, storage, and networking components, rack spaces, power, internet, and cooling. It also includes the room that the equipment is housed in, the building location and its surroundings, and the processes that are in place for the guards, physical security staff, or guests that access these locations.

Protecting the physical layer encompasses how we create redundancy and resiliency in IT systems, and how we record and audit who accesses the building and systems. This could include gated fences, guard stations, video surveillance, logging visitors, and background checks. These physical controls should be in place for any company that utilizes its own private data center.

Although some of the considerations here may not seem related to an intrusion, it's important to remember that an attacker's goal is not always to access data. Sometimes, the objective is disruption, which is why redundancy and resiliency are mentioned in this section.

When utilizing Microsoft cloud services, the physical controls are Microsoft's responsibility. We will discuss shared responsibility for cloud security in the next section.

Identity and Access Layer

Since the provider is responsible for the physical controls within cloud services, **identity and access** become the first line of defense that a customer can configure and protect against threats. This is why statements such as "*Identity is the new control plane*" or "*Identity is the new perimeter*" have become popular when discussing cloud security. Even if your company maintains a private data center for the primary business applications, there is still a good chance that you are consuming a cloud application that uses your company identities or credentials. For this reason, having the proper controls in place, such as **multi-factor authentication** (**MFA**), **conditional access policies**, and **Microsoft Entra Identity Protection**, will help to decrease vulnerabilities and recognize potential threats before a widespread attack can take place.

Perimeter Security Layer

Within a private data center, where the company controls the internet provider connection terminations and has firewall appliances, intrusion detection and protection solutions, and DDoS protection in place and fully configured, the protection of the perimeter is a straightforward architecture.

When working within cloud providers, **perimeter security** takes on a different focus. The cloud providers have agreements with the internet providers that provide services to their data centers, and these providers terminate these connections within their own hardware. The company perimeter security then becomes more of a virtual perimeter to their cloud tenant, rather than a physical perimeter to the data center network facilities. The company now relies on the provider's ability to protect against DDoS attacks at the internet perimeter.

Within Microsoft, DDoS protection is a free service since Microsoft wants to avoid a DDoS attack that would bring down many customers in a data center. For additional perimeter protection, the company can implement virtual firewall appliances to protect the tenant perimeter, to block port- and packet-level attacks, and additional solutions, such as Application Gateway, with a **web application firewall** (**WAF**) to protect from application-layer attacks.

Network Security Layer

The **perimeter** and **network security** layers work closely together. Both focus on the network traffic aspect of the company infrastructure. Where perimeter security handles the internet traffic that is entering the tenant, or data center, network security solutions protect how and where that traffic can be routed once it passes through the perimeter. Once an attacker can gain access to a system on the network, they will want to find ways to move laterally within the network infrastructure. Having proper IP address and network segmentation on the network can protect against this lateral movement taking place.

On a private data center network, this can be accomplished within switch ports with **virtual local area networks** (**VLANs**), configured to block traffic between network segments. In a cloud provider infrastructure, virtual networking, or VNETs, can accomplish similar network segmentation. In an Azure infrastructure, **network security groups** and **application security groups** can also be configured on network interfaces with additional port, IP address, or application-layer rules for how traffic can be routed within the network.

Compute Layer

After network security, we begin to get into the resources that hold our data. The first of these is our **compute** resources. To maintain clarity, we will generalize the compute layer as the devices with an operating system, such as Linux or Windows. Compute resources also include platform-based services where the compute layer is managed by the cloud provider, such as Azure App Service, Azure Functions, or containers. Within your own private data center with equipment that you own, protecting the host equipment and avoiding exposure by hardening the virtual hypervisor is necessary. In the public cloud, Microsoft or another cloud provider will be responsible for this. The customer responsibility for virtual machines in the cloud is focused on maintaining regular application of software updates and security fixes (often referred to as *patching*), to prevent exploitable vulnerabilities within the operating system. In addition, encrypting virtual machine operating systems and disks with Azure Disk Encryption will protect the disk images and contents from being exposed.

A common attack at the compute layer is scanning and gaining access to management ports on devices. Not exposing these ports, `3389` for Windows **Remote Desktop Protocol** (**RDP**) and `22` for the Linux **Secure Shell** (**SSH**) protocol, to the internet will provide a layer of protection against these attacks. Within Microsoft Azure, this can be accomplished with **network security group** rules, removing public IP addresses on virtual machines, **bastion hosts**, and/or utilizing **just-in-time virtual machine access**. Many of these security options will be discussed in *Chapter 7, Design a Strategy for Securing Server and Client Endpoints*.

Application Layer

The layer of defense that is closest to our data is our **applications**. Applications present data to users through our internet websites, intranet sites, and our line of business applications that are used to perform our day-to-day business. A cybersecurity architect will determine how to protect applications against common threats, such as cross-site scripting on our websites. To protect against these common threats, a WAF can be used for proper evaluation of the traffic accessing our applications. Using **Transport Layer Security** (**TLS**) protocol encryption can also help avoid the exposure of sensitive data to unauthorized individuals.

Prior to an application being moved to production, it should be rigorously tested to make sure that there are no open management ports and that all API connections are also secured.