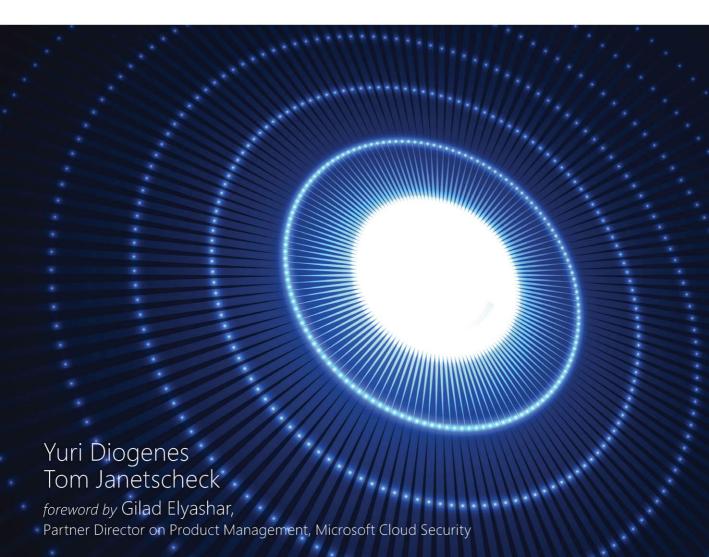


Microsoft Defender for Cloud





Microsoft Defender for Cloud

Yuri Diogenes and Tom Janetscheck

Microsoft Defender for Cloud

Table of Contents

1	$\widehat{}$	\sim	١	,	Δ	r
١			•	,	_	

Title Page

Copyright Page

Contents at a Glance

Contents

Acknowledgments

About the authors

Foreword

Introduction

Chapter 1 The threat landscape

The state of cybercrime

Understanding the cyberkill chain

Using the MITRE ATT&CK Framework to protect and detect

Common threats

Improving security posture

Adopting an assume-breach mentality

Cloud threats and security

Compliance

Risk management

Identity and access management

Operational security

Endpoint protection

Data protection



Azure security

VM protection

Network protection

Storage protection

Identity

Logging

Container security

Chapter 2 Planning Microsoft Defender for Cloud adoption

Deployment scenarios

Understanding Defender for Cloud

Defender for Cloud architecture

Defender for Cloud dashboard

Planning adoption

Considerations for CSPM

Considerations for CWPP

Considerations for multi-cloud

Considerations for vulnerability assessment

Considerations for EDR

Considerations for multi-tenant

Chapter 3 Onboarding Microsoft Defender for Cloud

Planning your Azure environment for Defender for Cloud

Designing your environment

Onboarding VMs from an Azure subscription

Understanding auto-provisioning

Auto provision the Log Analytics agent for Azure VMs

Deploy the Log Analytics agent to Azure Arc machines

Auto-provisioning of vulnerability assessment solutions

Auto-deployment of guest configuration agent



Deploy Microsoft Defender for Containers components

Connecting to Amazon Web Services (AWS)

Onboard AWS VMs

How to onboard subscriptions at scale

Registering the Microsoft.Security resource provider

Assign the Azure security Benchmark

Configure auto-provisioning at scale

Chapter 4 Policy management

Introduction to Azure Policy

Policy exemptions

Understanding Azure Security Benchmark

Fine-tuning policies in Defender for Cloud

Creating custom policies in Microsoft Defender for Cloud

Policy enforcement and governance

How to overcome reactive security management

Prevent security misconfigurations with Defender for Cloud

Large-scale provisioning with Azure Blueprints

Policy deployment and best practices

Regulatory standards and compliance

Regulatory compliance in Microsoft Defender for Cloud

Customize your regulatory compliance experience

Build your own compliance initiative

Creating custom assessments for AWS and GCP

Chapter 5 Strengthening your security posture

Driving security posture improvement using Secure Score

Fine-tuning your Secure Score

Using APIs and Continuous Export to create reports

Get Secure Score data



Secure Score over time report

Notify on Secure Score downgrade

Remediating recommendations

Enable multi-factor authentication (MFA)

Recommendations and controls focused on compute

Networking

Data and storage

Using workflow automation to remediate security recommendations

Resource exemptions and automation

Security governance and contextual security

Using security governance to create responsibility

Using Attack Paths to focus on the right resources

Build your own views with Cloud Security Map

Chapter 6 Threat detection

Methods of threat protection

Understanding alerts

Accessing security alerts

Alert suppression

Alerts in Azure Resource Graph (ARG)

Defender for Servers

Windows

Linux

Defender for Containers

Vulnerability Assessment

Threat detection

Defender for App Service

Defender for Storage

Considerations before enabling Defender for Storage



Defender for SQL

Vulnerability Assessment for SQL

Defender for Cosmos DB

Defender for Open-Source Relational Databases

Defender for Key Vault

Defender for Resource Manager

Defender for DNS

The cyberkill chain and fusion alerts

Threat intelligence in Defender for Cloud

Responding to alerts

Contact

Mitigation

Impact

Take action

Chapter 7 Better together

Defender for Cloud and Microsoft Sentinel

Integration with Microsoft Sentinel

Accessing alerts in Microsoft Sentinel

Defender for Cloud and Microsoft Purview

Defender for Cloud and Microsoft Defender for Endpoint

Chapter 8 Enhanced security capabilities

Just-in-time virtual machine access

Recommendation to enable JIT

JIT dashboard

Requesting access

File integrity monitoring

Customizing your settings

Visualizing changes



Configuring Adaptive Application Control

Chapter 9 Accessing Defender for Cloud from APIs

Understanding REST API

Accessing alerts using the Defender for Cloud REST API

Accessing alerts using the Graph Security API

Using the Graph Security API

Chapter 10 Deploying Microsoft Defender for Cloud at scale

The three cornerstones of deployment at scale

Defender for Cloud, Azure Policy, and Management Groupsbetter together

Best practices for managing Defender for Cloud at scale

How to get started with ARM templates

Export templates from the Azure portal

Use Visual Studio Code to create ARM templates

Appendix Microsoft Defender for DevOps

Shift left

Understanding Defender for DevOps

Connect your source code management system to Defender for Cloud

Configure pull request annotations

Discover security issues when developers commit code

Discover security issues in Infrastructure as Code (IaC)

Discover security issues during development

Index

