Contents at a Glance

Introduction 1

Part 1: Getting Started with Cloud Security 5

CHAPTER 1: Clouds Aren't Bulletproof 7
CHAPTER 2: Getting Down to Business 27
CHAPTER 3: Storing Data in the Cloud 43
CHAPTER 4: Developing Secure Software 65
CHAPTER 5: Restricting Access 95

Part 2: Acceptance 125

CHAPTER 6: Managing Cloud Resources 127
CHAPTER 7: The Role of AIOps in Cloud Security 145
CHAPTER 8: Implementing Zero Trust 173
CHAPTER 9: Dealing with Hybrid Cloud Environments 195
CHAPTER 10: Data Loss and Disaster Recovery 219

Part 3: Business as Usual 241

CHAPTER 11: Using Cloud Security Services 243
CHAPTER 12: When Things Go Wrong 265
CHAPTER 13: Security Frameworks 289
CHAPTER 14: Security Consortiums 311

Part 4: The Part of Tens 323

CHAPTER 15: Ten Steps to Better Cloud Security 325
CHAPTER 16: Cloud Security Solutions 335

Index 341

COPYRIGHTED MATERIAL

Table of Contents

INTRODUCTION 1
About This Book 2
Foolish Assumptions 3
Icons Used in This Book 3
Beyond the Book 3
Where to Go from Here 4

PART 1: GETTING STARTED WITH CLOUD SECURITY 5

CHAPTER 1: Clouds Aren't Bulletproof 7
Knowing Your Business 8
Discovering the company jewels 8
Initiating your plan 8
Automating the discovery process 8
Knowing Your SLA Agreements with Service Providers 10
Where is the security? 10
Knowing your part 11
Building Your Team 11
Finding the right people 12
Including stakeholders 12
Creating a Risk Management Plan 13
Identifying the risks 14
Assessing the consequences of disaster 15
Pointing fingers at the right people 15
Disaster planning 16
When Security Is Your Responsibility 17
Determining which assets to protect 17
Knowing your possible threat level 20
Van Gogh with it (paint a picture of your scenario) 21
Setting up a risk assessment database 22
Avoiding Security Work with the Help of the Cloud 24
Having someone else ensure physical security 25
Making sure providers have controls to separate customer data 25
Recognizing that cloud service providers can offer better security 25

CHAPTER 2: Getting Down to Business 27
Negotiating the Shared Responsibility Model 28
Coloring inside the lines 29
Learning what to expect from a data center 29
Taking responsibility for your 75 percent 31

SaaS, PaaS, IaaS, AaaA! 31
SaaS 31
SaaS security 32
PaaS 32
PaaS security 33
IaaS 33
IaaS security 34
FaaS 34
SaaS, PaaS, IaaS, FaaS responsibilities 34
Managing Your Environment 35
Restricting access 36
Assessing supply chain risk 36
Managing virtual devices 38
Application auditing 38
Managing Security for Devices Not Under Your Control 39
Inventorying devices 39
Using a CASB solution 40
Applying Security Patches 41
Looking Ahead 42

CHAPTER 3: **Storing Data in the Cloud** 43
Dealing with the Data Silo Dilemma 44
Cataloging Your Data 45
Selecting a data catalog software package 46
Three steps to building a data catalog 46
Controlling data access 47
Working with labels 49
Developing label-based security 50
Applying sensitivity levels 50
Assessing impact to critical functions 50
Working with Sample Classification Systems 51
Tokenizing Sensitive Data 54
Defining data tokens 54
Isolating your tokenization system 55
Accessing a token system 55
Segmenting Data 56
Anonymizing Data 56
Encrypting Data in Motion, in Use, and at Rest 58
Securing data in motion 59
Encrypting stored data 59
Protecting data in use by applications 60
Creating Data Access Security Levels 60

Controlling User Access 61
Restricting IP access 61
Limiting device access. 62
Building the border wall and other geofencing techniques 63
Getting rid of stale data 64

CHAPTER 4: **Developing Secure Software** 65
Turbocharging Development. 65
No more waterfalls 66
CI/CD: Continuous integration/continuous delivery. 68
Shifting left and adding security in development. 68
Tackling security sooner rather than later. 69
Putting security controls in place first 70
Circling back 70
Implementing DevSecOps 71
Automating Testing during Development 71
Using static and dynamic code analysis. 72
Taking steps in automation 73
Leveraging software composition analysis 74
Proving the job has been done right 76
Logging and monitoring 76
Ensuring data accountability, data assurance, and data dependability. 77
Running Your Applications. 78
Taking advantage of cloud agnostic integration. 79
Recognizing the down sides of cloud agnostic development 80
Getting started down the cloud agnostic path 81
Like DevOps but for Data 82
Testing, 1-2-3 84
Is this thing working? 85
Working well with others 85
Baking in trust 85
DevSecOps for DataOps. 86
Considering data security. 87
Ending data siloes 88
Developing your data store 89
Meeting the Challenges of DataSecOps. 90
Understanding That No Cloud Is Perfect 92

CHAPTER 5: **Restricting Access** 95
Determining the Level of Access Required 95
Catching flies with honey 96
Determining roles 97
Auditing user requirements. 97

Understanding Least Privilege Policy 98
Granting just-in-time privileges 99
The need-to-know strategy 99
Granting access to trusted employees 99
Restricting access to contractors 100
Implementing Authentication 101
Multifactor authentication (Or, who's calling me now?) 101
Authenticating with API keys 102
Using Firebase authentication 102
Employing OAuth 103
Google and Facebook authentication methods 103
Introducing the Alphabet Soup of Compliance 104
Global compliance 104
Complying with PCI 105
Complying with GDPR 106
HIPAA compliance 107
Government compliance 109
Compliance in general 110
Maintaining Compliance and CSPM 110
Discovering and remediating threats with CSPM applications 112
Automating Compliance 113
Integrating with DevOps 113
Controlling Access to the Cloud 114
Using a cloud access security broker (CASB) 115
Middleware protection systems 117
Getting Certified 121
ISO 27001 Compliance 121
SOC 2 compliance 122
PCI certification 124

PART 2: ACCEPTANCE 125

CHAPTER 6: **Managing Cloud Resources** 127
Defending Your Cloud Resources from Attack 128
Living in a Virtual World 129
Moving to virtualization 130
Addressing VM security concerns 130
Using containers 131
Securing Cloud Resources with Patch Management 132
Patching VMs and containers 133
Implementing patch management 133
Keeping Your Cloud Assets Straight in Your Mind 134
Keeping Tabs with Logs 136
Using Google Cloud Management software 136
Using AWS log management 137

Using Azure log management 139
Working with third-party log management software 139
Logging containers 140
Building Your Own Defenses 141
Creating your development team 141
Using open-source security 142
Protecting your containers 143
Protecting your codebase 143

CHAPTER 7: **The Role of AIOps in Cloud Security** 145
Taking the AIOps Route 146
Detecting the problem 148
Using dynamic thresholds 149
Catching attacks early in the Cyber Kill chain 149
Prioritizing incidents 150
Assigning tasks 150
Diagnosing the root problem 151
Reducing time to MTTR 151
Spotting transitory problems 152
Digging into the past 152
Solving the problem 153
Achieving resolution 154
Automating security responses 154
Continually improving 155
Making Things Visible 155
Implementing resource discovery 155
Automating discovery 156
Managing Resources, CMDB-Style 157
Seeing potential impacts 157
Adding configuration items 158
Employing CSDM 158
Using AIOps 159
Gaining insights 159
Examining a wireless networking use case 159
Using Splunk to Manage Clouds 161
Observability 161
Alerts 162
Splunk and AIOps 163
Predictive analytics 163
Adaptive thresholding 163
Views of everything 164
Deep Dive in Splunk 164
Event Analytics in Splunk 164
Splunk On-Call 165
Phantom 166

Putting ServiceNow Through Its Paces 167
AIOps require an overhead view 167
React to problems 167
Gauge system health 168
Automation makes it all happen 169
Getting the Job Done with IT Service Management 170
How ITSM is different 170
Performance analytics 170
Changing Your Team 171
A (Not So Final) Word 172

CHAPTER 8: **Implementing Zero Trust** 173
Making the Shift from Perimeter Security 174
Examining the Foundations of Zero Trust Philosophy 175
Two-way authentication 175
Endpoint device management 176
End-to-end encryption 177
Policy based access 179
Accountability 181
Least privilege 182
Network access control and beyond 182
CSPM risk automation 184
Dealing with Zero Trust Challenges 185
Choose a roadmap 186
Take a simple, step-by-step approach 186
Keep in mind some challenges you face in implementing zero trust 190

CHAPTER 9: **Dealing with Hybrid Cloud Environments** 195
Public Clouds Make Pretty Sunsets 196
Controlling your environment 197
Optimizing for speed 197
Managing security 198
Private Clouds for Those Special Needs 199
Wrapping Your Mind around Hybrid Cloud Options 200
Hybrid storage solution 201
Tiered data storage 202
Gauging the Advantages of the Hybrid Cloud Setup 203
It's scalable 203
The costs 203
You maintain control 203
The need for speed 204
Overcoming data silos 204
Compliance 206

Struggling with Hybrid Challenges 207
Handling a larger attack surface 207
Data leakage 207
Data transport times 208
Complexity 208
Risks to your service level agreements 208
Overcoming Hybrid Challenges 209
Asset management 209
SAM 210
HAM 211
IT asset management 211
Latency issues 212
On the Move: Migrating to a Hybrid Cloud 213
Data migration readiness 213
Making a plan 213
Picking the right cloud service 214
Using a migration calendar 215
Making it happen 215
Dealing with compatibility issues 215
Using a Package 216
HPE Hybrid Cloud Solution 216
Amazon Web Services 216
Microsoft Azure 217

CHAPTER 10: **Data Loss and Disaster Recovery** 219
Linking Email with Data Loss 220
Data loss from malware 221
The nefarious ransomware 222
Ransomware and the cloud 223
Crafting Data Loss Prevention Strategies 224
Backing up your data 226
Tiered backups 226
Minimizing Cloud Data Loss 229
Why Cloud DLP? 229
Cloud access security brokers 229
Recovering from Disaster 232
Recovery planning 232
Business continuity 232
RTO and RPO 233
Coming up with the recovery plan itself 233
Chaos Engineering 235
Practical chaos engineering 236
Listing what could go wrong 238
Seeing how bad it can get 239
Attaining resiliency 239

PART 3: BUSINESS AS USUAL 241

CHAPTER 11: Using Cloud Security Services 243
Customizing Your Data Protection 244
Validating Your Cloud 244
Multifactor authentication 245
One-time passwords 245
Managing file transfers 250
HSM: Hardware Security Modules for the Big Kids 251
Looking at HSM cryptography 252
Managing keys with an HSM 253
Building in tamper resistance 255
Using HSMs to manage your own keys 255
Meeting financial data security requirements with HSMs 256
DNSSEC 256
OpenDNSSEC 257
Evaluating HSM products 258
Looking at cloud HSMs 259
KMS: Key Management Services for Everyone Else 259
SSH compliance 260
The encryption-key lifecycle 262
Setting Up Crypto Service Gateways 263

CHAPTER 12: When Things Go Wrong 265
Finding Your Focus 265
Stealing Data 101 266
Landing, expanding, and exfiltrating 267
Offboarding employees 273
Preventing the Preventable and Managing Employee Security 276
Navigating Cloud Native Breaches 280
Minimizing employee error 281
Guarding against insider data thefts 283
Preventing employee data spillage 284
Cleaning up after the spill 285

CHAPTER 13: Security Frameworks 289
Looking at Common Frameworks 290
COBIT 290
SABSA 291
Federal Financial Institutions Examination Council (FFIEC) Cyber Assessment Tool (CAT) 292
Federal Risk and Authorization Management Program (FEDRAMP) 292
Personal Information Protection and Electronic Documents Act (PIPEDA) 293

Payment Card Industry — Data Security Standard (PCI–DSS). . . .293
GLBA 293
SCF 294
DFARS 252.204-7012/ NIST 800-171 294
ISO/IEC 27000 Series 295
CIS Critical Security Controls 295
CIS Benchmarks 295
Common Criteria 296
FDA regulations on electronic records and signatures 296
ITIL 297
Introducing SASE Architecture 298
The sassy side of SASE 299
Sassy makeup 300
The Cloud Native Application Protection Platform 303
Working with CWPP 304
Managing with CSPM 305
NIST Risk Management Framework 305
Federal Information Security Modernization Act 306
Cybersecurity Strategy and Implementation Plan 307

CHAPTER 14: **Security Consortiums** 311
Doing the Right Thing 311
Membership in the Cloud Security Alliance 313
Company membership 314
Individual membership 315
Getting that Stamp of Approval 317
CCSK Certification 317
CISA: Certified Security Information Systems Auditor 317
CRISC: Certified Risk and Information Systems Control 318
CCAK: Certificate of Cloud Auditing Knowledge 318
Advanced Cloud Security Practitioner 318
GDPR Lead Auditor and Consultant 319
Information Security Alliances, Groups, and Consortiums 319
Words for the Road 321

PART 4: THE PART OF TENS 323

CHAPTER 15: **Ten Steps to Better Cloud Security** 325
Scoping Out the Dangers 326
Inspiring the Right People to Do the Right Thing 327
Keeping Configuration Management on the Straight and Narrow 328
Adopting AIOps 329
Getting on board with DataOps 330
Befriending Zero Trust 330

Keeping the Barn Door Closed 331
Complying with Compliance Mandates 332
Joining the Cloud Security Club 333
Preparing for the Future 333

CHAPTER 16: **Cloud Security Solutions** 335
Checkpoint CloudGuard 335
CloudPassage Halo 336
Threat Stack Cloud Security Platform 336
Symantec Cloud Workload Protection 336
Datadog Monitoring Software 337
Azure AD 338
Palo Alto Prisma 338
Fortinet Cloud Security 338
ServiceNow AIOps 339
Lacework 340

INDEX 341