Zero Trust in Resilient Cloud and Network Architectures

JOSH HALLEY
DHRUMIL PRAJAPATI
ARIEL LEZA
VINAY SAINI

ciscopress.com

Zero Trust in Resilient Cloud and Network Architectures

Josh Halley, CCIEx3 No. 11924

Dhrumil Prajapati, CCIEx2 No. 28071,
CCDE No. 20210002

Ariel Leza

Vinay Saini, CCIE No. 38448,
CWNE No. 69, CCDE No. 20240032

Cisco Press

Zero Trust in Resilient Cloud and Network Architectures

Table of Contents

Cover

Title Page

Copyright Page

Contents at a Glance

Contents

Introduction

Chapter 1 Zero Trust Demystified

- Definition of Zero Trust
- How It All Began
- Why We Need Zero Trust
- Core Principles of Zero Trust
  - Explicit Verification
  - Least-Privilege Access
  - Assume Breach
- Major Zero Trust Industry Standards
- People, Processes, and Technology
  - People
  - Processes
  - Technology
- On-Premises vs. Cloud
  - Explicit Verification
  - Least-Privilege Access

Pearson

Table of Contents

- Segmentation
- Continuous Monitoring and Threat Detection
- Encryption and Data Protection
- Automated Response and Orchestration
- Endpoint Security
- Incident Response and Recovery
- Policy Enforcement

Hybrid Environment Recommendations

Security Certifications

Summary

References

Chapter 2 Secure Automation and Orchestration Overview

Introduction to Automation and Orchestration

- Evolution of Network Automation
- Network Maturity for Automation

Building Blocks of Secure Automation

- Secure Automation with API Security
- Dynamic Application Security Testing (DAST)
- Integrating XDR, SIEM, and SOAR

Common Automation Practices and Tools

- Orchestration Using Ansible
- Orchestration Using Terraform
- CI/CD/CT

AI and Machine Learning with Automation

- Machine Learning (ML)
- Neural Networks
- Generative AI and LLMs
- Data Lakes

Table of Contents

Summary

Chapter 3 Zero Trust Network Deployment

Elements of Zero Trust Strategy Definitions

Establishing Trust

User Trust Definition

Device Trust Definition

Trust Score Calculation

Defining Application Access Policies

Enforcing Policies

Contextual Data

Connection Metadata

Logging Suspicious Actions

Trust Tolerance

Tools and Technologies

Central Inventory

Identity and Access Management

Network Segmentation

Device Posture with Endpoint Security

Virtual Private Network (VPN)

Identifying Business Workflows

Applying Zero Trust Using SSE

Client-Based ZTNA Deployment for Managed Corporate Devices

Clientless ZTNA Deployment for Unmanaged Devices

VPN-Based ZTNA Using SSE

SSE Integration for IoT Devices Using SD-WAN

ZTNA Deployment Scenarios

Greenfield ZTNA Deployment

Brownfield ZTNA Deployment

Summary

Table of Contents

Chapter 4 Security and Segmentation

- Overview
- Segmentation Options
  - Governance Considerations
  - Macrosegmentation
  - Routing Paths
  - Stateful Inspection
  - Audit Trail
  - Failure Domain
  - Microsegmentation
  - Best Practices for Macro- and Microsegmentation
  - Verification of Security Group Tags on IOS XE Platforms
- Methods of TrustSec Transport
  - CTS Inline Tagging
  - VXLAN Encapsulation
  - GRE Encapsulation
  - IPsec Encapsulation
- Control Plane TrustSec Transport
  - SXP
  - LISP
  - Static
  - SGT Priority Order
  - Secure Service Insertion
  - LAN-to-Cloud Microsegmentation
- Summary

Chapter 5 DHCP and Dynamic Addressing Concepts

- Introduction to Dynamic Addressing
- Zero Trust Approach to Dynamic Addressing

Table of Contents

Rogue DHCP Servers
DHCP Starvation
DHCP Man in the Middle
DHCP Options
DHCP Authentication
IPv6 Address Assignment
Well-Known Multicast
Transient Multicast IPv6 Addresses
Neighbor Discovery in IPv6
Solicited-Node Multicast Addresses
Anycast Addresses
Address Assignment in IPv6
DHCPv6 Options
IPv6 First Hop Security
Rogue RA
DHCPv6 Guard
IPv6 Destination Guard
Source Guard and Prefix Guard
RA Throttle
ND Suppress Multicast
Summary
Chapter 6 Automating the Campus
Overview
Planning
IP Addressing
Underlay Infrastructure IP Addresses
Management IP Addresses
Overlay User IP Addresses
Maintaining IP Addressing Continuity

Table of Contents

Site Hierarchy

Execution

LAN Automation

LAN Automation Process and Workflow

API-Based LAN Automation Provisioning

Partial Automated Deployment

Summary

References

Chapter 7 Plug-and-Play and Zero-Touch Provisioning

Overview

Plug-and-Play Provisioning

Cisco Catalyst Center Call Flow

Certificates

Time Management

Using IPv4 DHCP to Perform Plug-and-Play

DHCP Server Scope

DNS Server: DHCP Option 6

Domain Name: DHCP Option 15

Vendor Class Identifier: DHCP Option 60

DHCP Option 43

Using DNS to Perform Plug-and-Play

Plug-and-Play Connect

Startup VLAN

LACP Usage with PnP

Authorization of PnP Devices

Meraki Onboarding Flow

Zero-Touch Provisioning

Foundation Configurations

Software and Hardware Deployment Selection in Catalyst Center

Table of Contents

Claiming Devices in Catalyst Center

Claiming Devices in the Meraki Dashboard

Template Usage in Catalyst Center

Standard Templates

Composite Templates

Bouncing Interfaces

Programmability-Based Deployment

Using Direct API Calls to Claim Devices

Claiming Devices Using Ansible

Customer Use Cases

Large Banking Customer: Pan-Africa Deployment

Global Deployment: Large-Scale Enterprise Deployment

Summary

Chapter 8 Routing and Traffic Engineering

Overview

Routing

Underlay Routing Protocols

Enhanced Interior Gateway Routing Protocol (EIGRP)

OSPF

IS-IS

Overlay Routing Protocols

MPLS-VPN

BGP-EVPN

SD-Access

ACI

SD-WAN

Traffic Engineering

Network Design

Routing Protocols

Table of Contents

Traffic Flow Analysis

Traffic Management

Load Balancing and Sharing

Quality of Service

Bandwidth Planning, Congestion, and Oversubscription

Network Monitoring and Optimization

Policy and Security

Global Internet

Geo-routing

Summary

References

Chapter 9 Authentication and Authorization

Overview

A Broader View of Identity

Authentication and Authentication Methods

Local Authentication

Centralized ServerBased Authentication

Service Accounts

When Using Service Accounts Goes Wrong

x.509 Certificate-Based Authentication

REST-API Authentication Methods

Multifactor Authentication (MFA)

Network Access Control

MAC Authentication Bypass

802.1x (Network Authentication)

Authorization

Dynamic Change of Authorization (CoA)

Identifying and Mitigating Risks of Unmaintained Virtual Machines in Network Access Control Deployments

Table of Contents

Monitoring Authorization Health

Customer Use Cases

Using Dynamic Policy to Improve Real-World Challenges

Expediting System and Workstation Patches

Summary

Chapter 10 Quantum Security

What Is Quantum Computing?

The Need for New Computing Technologies

How Quantum Computing Is Different

Quantum Superposition

Qubit Modalities

Quantum Entanglement

Gate Operations

H Gate

CNOT Gate

Current State

Quantum Computing and Emerging Security Threats

Shors Quantum Algorithm

Grovers Algorithm

Why Worry Now?

Approaches to Safeguard Against Quantum Adversaries

Symmetric Keys

Quantum Key Distribution

Practical Solution Approach

Quantum-Safe IPsec

Quantum-Safe MACsec

Dynamic Keys

Summary

Chapter 11 Network Convergence and Considerations

Table of Contents

- What Is Convergence?
- Convergence in Layer 3 Routed Architectures
  - Protocol Convergence Timers
  - Server-Side Verification
  - Convergence in Data Center Networks
  - Convergence in Software-Defined Architectures
- Methodologies of Convergence Testing
  - Simulating Routed Convergence Scenarios
  - What Is Stateful Mode?
  - What Is Stateless Mode?
- Monitoring Security Convergence
- Summary

Chapter 12 Software-Defined Network Deployment Best Practices

- Introduction
- Network Deployment Lifecycle
- Stage 1: Planning and Design
  - Defining Network Requirements and Use Cases
  - Selecting the Right SDN Architecture
  - On-Premises Controller
  - Software-as-a-Service (SaaS) Controllers
  - Reviewing the Key Characteristics of SDN Controllers
  - Designing a Robust Network Topology
  - Addressing Security Considerations in SDN
  - Planning for Multidomain and Cloud Integration
- Stage 2: Deployment and Migration
  - Preparing the Network Infrastructure
  - Deploying the SDN Controller

Table of Contents

Installing and Configuring the SDN Controller

Setting Up High Availability and Disaster Recovery

Prioritizing Network Services for SDN Migration

Testing and Validating Migration Success

Stage 3: Operations and Management

Integrating SDN Automation with Existing IT Operations Management Systems

Monitoring and Troubleshooting the SDN Environment

Maintaining Security and Compliance

Summary

References

Chapter 13 Wired and Wireless Assurance

What Is the Best Practice for Your Enterprise Architecture?

Wired Network Best Practice Design Concepts

Tiered Network Design

Stacking Constructs

Layer 3 Architectures

Optimizing Wireless Networks

Central Tunneling of Traffic (Over the Top)

Local Breakout

Anchoring Concepts (Catalyst/Meraki)

Monitoring TrustSec and Security Enforcement

Case Study: Financial Sector Customer

Summary

Chapter 14 Large-Scale Software-Defined Network Deployment

Introduction

Network Design

Physical Hardware: Bill of Materials

Table of Contents

Layer 2: Local Area Network

Layer 3: Local Area Network

Secure Connect: Wide Area Network

Ordering and Delivery

Security

MX Security Features

Security in Action

ISE Integration

Dynamic VLAN Assignment Case Study

Adaptive Policy Microsegmentation

Security Configuration

Automation

Meraki as Code

Using Git for Configuration Management

CI/CD Pipeline

Fast Burger Automation

Implementation: Kyle and Jason Go to Fast Burger

Summary

Chapter 15 Cloud-Native Security Foundation

Introduction to Cloud-Native Security: A Zero Trust Perspective

From Cloud Infrastructure to Cloud Native: An Introduction to Cloud- Native Architectures

Characteristics of Cloud-Native Architectures: What Makes It Different?

Foundations of Cloud-Native Architectures

Containerization: The Building Blocks

Microservices Architecture: The Core of Modularity

Dynamic Orchestration and Management

Integrating DevOps and DevSecOps

Immutable Infrastructure and Scalability

Agility and Scalability: The Heartbeat of Cloud Native

Table of Contents

Resiliency: Designing for Failure

API-Based Communication: Facilitating Service Interoperability

Observability: Insight into Cloud-Native Systems

Security: A Foundational Pillar

Building a Comprehensive Cloud-Native Security Strategy

Core Principles of Cloud-Native Architectures and Security

Why Microservices and Immutability Enhance Security

Service-to-Service Communication vs. Traditional Centralized Firewall

Cloud Infrastructure Security: Pillars and Practices in the Modern Cloud

The Shared Responsibility Model: A Foundation of Cloud Security

Architectural Foundations of Cloud Security in Hyperscaler Platforms

Unified Security Models and Identity and Access Management (IAM)

Data Encryption and Protection

Network and Infrastructure Security

Implementing Automated Compliance and Governance

Security Monitoring: Threat Detection and Response

Key Management in Cloud Environments

Understanding Key Management Systems (KMS) in the Cloud

Benefits of Using KMS

Best Practices for Cloud-Based Key Management

HashiCorp Vault: A Cloud-Native Key Management Solution

Components and Architecture of HashiCorp Vault

Network Security Evolution and Segmentation

Infrastructure as Code (IaC) and Security Automation

Advanced Load Balancing and Application Layer Security

Application Load Balancers (ALBs): Features and Use Cases

The Future Landscape: Why OSS ALBs and Ingress Controllers Are Gaining Traction

The Cloud-Native Security Stack: From Infrastructure to Application

Table of Contents

Navigating Multicloud and Hybrid Cloud Security

Advanced Security Measures and Third-Party Services

The Need for Cloud Security Posture Management (CSPM)

Features of CSPM

Benefits of CSPM

The Future of CSPM

Integrating Cisco Solutions: Enhancing Multicloud and Hybrid Cloud Security with Attack Surface Management and JupiterOne

Cloud Workload Protection Platforms (CWPPs) and Cisco Secure Workload

Relationship to Zero Trust

Going Up the Stack from Infrastructure to Application

Monitoring and Logging Requirements for Compliance

Ensuring Visibility and Transparency Across the Cloud-Native Stack

Leveraging OpenTelemetry for Security

Splunk for Enhanced Security Posture

Continuous Monitoring and Automation Regulatory Requirements and Compliance Standards

Emerging Trends and Technologies in Cloud-Native Security

The Role of AI and ML in Enhancing Security Postures

Enhancing Security with AI/ML: A Practical Cisco Scenario

Anticipating Future Threats and Preparing Defenses

Embracing Continuous Threat Exposure Management (CTEM) for Enhanced Cybersecurity

More Than Vulnerability Management Evolution: Why CTEM Is Gaining Traction

Getting Started with CTEM

The Evolving Landscape of Cloud-Native Security Standards and Framework

Incorporating Matured Zero Trust Frameworks into Cloud-Native Security

DISA Zero Trust Framework

CISA Zero Trust Maturity Model V2.0

NIST Special Publication 800-207Zero Trust Architecture

Table of Contents

Cisco Zero Trust Framework

The Role of Zero Trust Frameworks in Evolving Cloud-Native Security

The Cisco SAFE Security Reference Model

Summary

References

Chapter 16 Cloud-Native Application Security

Introduction to Cloud-Native Application Security

Definition and Scope

Key Challenges

Evolution from Traditional Security

Understanding OWASP and Cloud-Native Security Risks

OWASP Top 10: Web vs. Cloud-Native

Expanding OWASP Principles for Cloud-Native Architectures

Should We Consider a Cloud-Native-Specific Model?

CNCF Projects for Cloud-Native Security

1. Provisioning

2. Runtime

3. Orchestration and Management

4. App Definition and Development

5. Observability and Analysis

6. Platforms

Top 20 CNCF Projects Focused on Security

Cloud

Clusters

Containers

Code

Role of Cloud-Native Application Protection Platform (CNAPP)

API Security

Vulnerability Management

Table of Contents

- Runtime Protection
- Policy Enforcement
- Compliance Management

Building Secure Applications with Cloud-Native Security

- Security in Application Design and Development
- Principle of Least Privilege
- Immutable Infrastructure
- Secrets Management
- Secure Coding Practices
- Shift-Left Security and DevSecOps Integration
- DevSecOps: Embedding Security into DevOps
- Top Cloud Security Risks in DevOps
- Strategies for Enhancing Collaboration
- Managing Dynamic Cloud Configurations
- Configuration Management Tools
- Continuous Monitoring and Drift Detection
- Dynamic Secrets Management
- Automated Remediation Tools
- Infrastructure as Code (IaC) and Security
- Securing the Software Supply Chain
- API Security
- Secure APIs Using Kubernetes Security

Unique Security Considerations for Serverless Architectures

- Serverless Shared Responsibility Model
- Key Serverless Security Challenges
- Function-Level Permissions
- Dependency Management
- API Gateway Security
- Visibility and Monitoring

Table of Contents

Proactive Threat Detection and Response

Data Leakage

The Path Forward for Serverless Security Best Practices

Enforce Fine-Grained Permissions

Manage Dependencies Proactively

Harden API Gateways

Enhance Visibility and Real-Time Monitoring

Protect Sensitive Data and Logs

Automate Security Validation and Compliance

Proactive Threat Detection and Response

Collaborative Security with DevSecOps

Adopt a Security-First Mindset with Automation

Critical Attack Vectors in Serverless Applications

Function Input Manipulation

Access Control and Authentication

Resource and Configuration Attacks

Event Injection

Cold Start Abuse

Other Common Security Risks Witnessed

Detailed Security Flow Through Components

1. User Request Initiation

2. API Gateway Processing

3. Function Trigger Evaluation

4. Permission Check Verification

5. Function Execution Management

6. Monitoring Layer

7. Data Services Integration

8. Security Scanning

Database Access Example

Emerging Trends and Future Outlook in Cloud-Native Security

Table of Contents

Reimagining Cloud Security and Zero Trust with CNAPP Solutions

Toward Proactive Cloud Security with CNAPP Solutions

Enhancing API Security with LLMs and CNAPP Solutions

Summary

References

Chapter 17 Data Center Segmentation On-Prem to the Cloud

Introduction to Data Center Segmentation in Hybrid and Multicloud Environments

The Limitations of Traditional Segmentation

A New Approach to Segmentation

Zero Trust and Microsegmentation Principles for Segmentation

What Is Zero Trust?

Key Benefits of Zero Trust

The Synergy of Zero Trust and Microsegmentation

Segmentation Challenges in Hybrid and Multicloud Environments

Inconsistent Policy Frameworks

Visibility and Compliance

Dynamic Workloads

Ways to Address These Challenges

Ways to Implement End-to-End Segmentation Policies with Zero Trust

Unified Policy Definition Across Domains

Workload-Specific Segmentation

Methods to Prevent Policy Drift

Core Features of Cisco Cloud Network Controller for Unified Segmentation

The Role of Zero Trust in Unified Policies

Ways to Migrate Segmentation Policies: From On-Premises to Cloud

Adapting Segmentation to Cloud-Native Architectures for Zero Trust Integration

Navigating the Transition from Cisco Cloud Controller

Overview of Policy Models: Cisco ACI and Cloud-Native Constructs

Table of Contents

- Cisco ACI Policy Model
- Cloud Policy Models (AWS, Azure, GCP)
- Comparison and Mapping of Policy Constructs
- Comparison to Cloud Segmentation Models
- Contracts as Security Policy Objects in Cisco ACI
- Provider-Consumer Model in Cisco ACI
- How Cisco ACI Contracts Simplify Network Management
- Effective Segmentation Migration Methods
- Phased Migration with Policy Layers
- Parallel Deployment for Hybrid Continuity
- Automated Policies for Rapid Big Bang Migrations
- Consistency Across Hybrid and Multicloud Environments
- How to Leverage Tenants for Multisite Management
- Consistent Policy Enforcement and Centralized Management
- Dynamic Policy Enforcement and Adaptation
- Operational Efficiency and Automation
- Multisite Application of Tenants
- How to Use a Multicloud Policy Orchestrator Across Clouds
- Open-Source Cross-Domain Orchestration and Automation for Segmentation Policies
- Integration of Open-Source Tools for Cross-Cloud Policy Consistency
- AI/ML for Adaptive Policy Enforcement in Hybrid Cloud Environments
- Visibility, Monitoring, and Predictive Analytics in Hybrid or Multicloud Environments

Web3 and Immutable Trust in Hybrid Cloud Segmentation

- What Is Web3?
- Web3 Technologies and Zero Trust: A Symbiotic Relationship
- How Decentralized Identity (DID) Works
- Hybrid Cloud Challenges and Web3s Role in Policy Enforcement
- Decentralized Identity: A Cornerstone of Web3 Security
- Ways to Enhance Security with Blockchains Immutability

Table of Contents

Security in Web3 and Smart Contracts

Blockchain for Immutable Access Logs

Web3s Value Beyond Blockchain: A New Security Paradigm

DID in Cloud-Native and Hybrid Environments

Real-World Applications of DID and Zero Trust

Workflow: Kubernetes Access Using DID and Smart Contracts

Coding Mistakes and Exploits

Latency Concerns

Smart Contract Revocation Challenges

Kubernetes Webhook Security Risks

Blockchain Cost and Scalability

Integrating Kubernetes with Blockchain for Smart ContractBased Access Control

Decentralized Identity Authentication in Kubernetes with Keycloak SPI

Authentication Flow Implementation Details for DID and Smart Contracts

User Initiates Authentication (Signing Challenge with Web3 Wallet)

Keycloak SPI Validates Signature and DID

The OIDC Token Is Issued

Kubernetes Validates the OIDC Token

Developer Uses Token to Access Kubernetes

Kubernetes Enforces Access Using Smart Contracts Authorization

External Admission Controller (Validating Webhook)

Kubernetes Enforces DID-Based Segmentation

Smart Contracts for Policy Enforcement

Solidity Contract Example

Audit Logging: Immutable Developer Access Logs

Benefits of This Approach

Summary

References

Table of Contents

Chapter 18 Using Common Policy to Enforce Security

Introduction to Security Policies

What Is a Cloud Security Policy?

Principles of Effective Policy Management

Designing Common Security Policies

Unifying Security Policy Frameworks

Balancing Granularity and Manageability

Standardizing Policies Across Diverse Environments

Creating Consistency Across Environments

Adapting to Changing Access Patterns with Common Policy

Policy Enforcement Mechanisms

Firewalls and Intrusion Detection/Intrusion Prevention Systems (IDS/ IPS)

Cloud Access Security Brokers (CASBs)

The Role of CASB in Cloud Security

Security Orchestration, Automation, and Response (SOAR)

CASB and SOAR: A Harmonious Approach

Identity and Access Management (IAM) Policies

Crafting Consistent IAM Policies

Role of Identity Federation and Single Sign-On (SSO)

Managing Privileged Access

Implementing Multicloud IAM

Data Protection and Privacy Policies

Aligning Data Governance with Security Policies

Ensuring Compliance with Regulations

Network Security Policies

Segmentation Policies for Network Security

Secure Network Configuration and Management Policies

From SDLC to SDL to SSDLC: A Journey Toward Secure Software Development

Table of Contents

- Software Development Life Cycle (SDLC): The Foundation of Application Development
- Origins of SDLC
- Phases of SDLC
- Security Threat and Vulnerability Assessment and Measurement in Secure Software Development
- Common Vulnerability Causes
- Taxonomy in Action Example
- Transitioning from SDLC to SDL: Embedding Security
- SDL Enhancements to SDLC Phases
- Why the Enhancements of SDL Are Beneficial
- Secure Software Development Lifecycle (SSDLC): Evolving with Agile and DevOps
- Key Enhancements in SSDLC
- Phases in SSDLC
- Benefits of SSDLC
- Understanding the Evolution of Software Development Security Frameworks
- Key Transition Milestones
- Framework Comparison

OWASP SAMM: A Framework for Security Maturity

- Understanding SAMMs Structure
- SAMM Framework Overview
- Governance: A Business Function in Focus
- How SAMM Relates to SDLC, SDL, and SSDLC
- Benefits and Implementation

Monitoring, Logging, and Auditing Policies

- Unified Logging and Continuous Monitoring
- Automated Auditing and Compliance Reporting

Incident Response and Remediation Policies

- Incident Response Frameworks

Table of Contents

Automated Policy-Based Remediation

Policy Compliance and Verification

Continuous Compliance Monitoring

Integrating Policy Checks into CI/CD Pipelines

Challenges in Policy Enforcement Across Hybrid Environments

Inconsistent Enforcement Capabilities

The Need to Overcome Resistance to Unified Frameworks

Future Directions in Policy-Based Security

Predictive and Adaptive Policies

The Role of AI in Dynamic Policy Management

Security Suites Delivered by the Cisco Security Cloud

Cisco User Protection Suite

Cisco Cloud Protection Suite

Cisco Breach Protection Suite

Summary

References

Chapter 19 Workload Mobility: On-Prem to Cloud

Definition and Scope of Workload Mobility

Is Your Cloud Ready for Your Workloads? Understanding the Benefits and Challenges

Real-World Application: ABC Corps Cloud Migration Journey

Motivations for Cloud Migration

Cost Efficiency and Budget Management

Innovation-Friendly and Fast Development Environment

Access to Advanced Computing Capabilities

Enhanced Security and Compliance

Focus on Core Business Activities

Global Reach and Market Expansion

Hybrid IT Infrastructure and Workload Placement

Table of Contents

On-Premises Infrastructure

Multicloud Strategy

Co-Location and Its Role in Modern IT Strategies

The Deployment of Cloud Smart on Hybrid IT Environments

Cloud Smart Environment for Workload Placement

Choosing a Cloud Model with Zero Trust as the Goal

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Software as a Service (SaaS)

Containers as a Service (CaaS)

Function as a Service (FaaS)

Analysis of TCO and ROI for Workload Migration

Migration Context

Moving Applications and Data

Deployment Model

People, Processes, and Technology

Building Out a Secure Migration Plan

Migration Strategies: From the Five to Seven Rs

Security Considerations for Data Transfer and Transition Phases

Integrating AWSs Well-Architected Framework: Case Study of ABC Corp

Building a Strong Identity Foundation

Maintaining Traceability

Applying Security at All Layers

Making Security Best Practices into Habits

Ensuring Data Is Protected in Transit and at Rest

Keeping People Away from Data

Preparing for Security Incidents

Performing Risk Assessment and Mitigation

Table of Contents

Embracing the AWS Shared Responsibility Model

Connecting with the Well-Architected Frameworks

Workload Migration Frameworks and Tools

Leveraging Migration Services and Tools

Understanding the Role of Automation and Integration

Ensuring Data Security During Migration

Optimizing Cloud Migration Outcomes

The What to Migrate

Comprehensive Tooling for Migration

Data Security During Workload Migration

Ensuring Data Integrity and Confidentiality

What Is Secure Data Transfer?

Types of Cloud Data Transfer

Online Data Migration

Network Data Transfers

Direct Connect Services

Hybrid Data Migration

Offline Data Migration

Considerations for Each Approach

Secure Data Transfer Best Practices

Data Transfer vs. Cloud Migration: An Overview

Data Transfer Considerations as Part of a Broader Cloud Migration Strategy

The Impact of Bandwidth Limitations

Tactics for Mitigating Bandwidth Limitations

Data Security Concerns

Downtime Risks

Compatibility Issues

Legacy Systems vs. Modern Cloud Infrastructure

Data Format and Structure

Table of Contents

- Use Cases in Cloud Migration
- Tools and Their Application in Cloud Migration
- Application Compatibility

Cloud Migration Security

- What Makes Migration to the Cloud Such a Necessity?
- What Is Cloud Migration Security?
- Risks of Cloud Migration
- Preparing for Cloud Migration Security Concerns
- API Vulnerabilities
- Security Blind Spots
- Compliance Requirements
- Data Loss
- Effective Safeguarding for Executing a Cloud Migration
- Understanding Your Data and Compliance Requirements
- Safeguarding APIs and Access Controls
- Encrypting Your Data During Transit
- Limiting Data Access During Cloud Migration
- Employing a Phased Migration Strategy and Risk Mitigation
- Implementing Decommissioning and Sanitization Activities
- Formulating a Security Plan
- Maintaining Data Protection and Integrity
- Confirming Security Measures
- Cloud Migration: Security Checklist
- Pre-Migration Security Preparations
- Security During Migration
- Post-Migration Security Maintenance

Quality Engineering: The Heart of Cloud Migration

- The Landscape of Cloud Migration Challenges
- Quality Engineerings Strategic Blueprint

Table of Contents

Ensuring Data Security and Navigating Cloud Migration with Precision

Network and Connectivity Considerations

The Maintenance of Network Security Postures During and After Migration

Continuous Monitoring and Assessment

Access Controls and Segmentation

Network Segmentation

Access Controls

Network Considerations for Cloud Migration

Measuring and Ensuring Network Performance

Consistently Measuring Network Performance

Measuring and Assessing Network Performance by Monitoring Key Metrics

Network Performance Measurement Tools

Application Dependency Mapping (ADM) and Application Performance Management (APM): Navigating Secure Cloud Migration and Zero Trust Architecture

ADM: Charting the Cloud Migration Terrain

APM: The Compass for Cloud Optimization

ADM and APM: Synergizing Security and Performance

Leveraging Hyperscaler Observability Tools for Strategic Cloud Integration

Core Benefits of ADM and APM Integration in Dynamic Cloud Environments

Integrating Observability into Cloud Migration

Key Outcomes

Metrics and Monitoring

The Role of OpenTelemetry and CNCF in Cloud Migration

Integrating OpenTelemetry into Network Measurements

Integration Approaches

A Real-World Example for Integrating OpenTelemetry into the Networking Domain

Tying It All Together

End-to-End Visibility on Digital Experience Using Cisco ThousandEyes

The Prologue: Setting the Stage for Migration

Table of Contents

The Journey: Navigating the Migration

The Finale: Validating Success

Managing IP Addressing and DNS Changes

Challenges in IP Planning

Best Practices for IP Planning

Designing Virtual Networks

Universal Best Practices Across Cloud Platforms

Best Practices for Virtual Networks Designs and Considerations During Cloud Migration

DNS

Ensuring High Availability and Disaster Recovery Readiness

Selecting a Cloud Provider and Service Model

Designing Your Cloud Architecture and Migration Strategy

Executing and Monitoring Migration and Disaster Recovery

Security Posture Adjustment Post-Migration

Adjusting Security Controls to the Cloud Environment

Monitoring and Responding to Security Events During the Stabilization Period

Updating Incident Response and Forensic Capabilities

Using Hyperscalers and Cisco-Provided Security Tools

Identity and Access Management in Hybrid Environments

IAM Basics

Significance of IAM in Hybrid Environments

Strategic Considerations for IAM in Hybrid Environments

IAM Role Mapping and Policy Enforcement

Federated Identity for Seamless Access Control

Privileged Access Management in a Hybrid Setting

Key IAM Migration Considerations

Best Practices and Considerations for IAM Implementation

How to Structure Resources and Permissions in the Cloud

Table of Contents

Permissions and IAM

Explanation and Context

External Access and Security Considerations

Guardrails and Automated Analysis

Automated Analysis Solutions

Summary

References

Chapter 20 Resilience and Survivability

Resilience Metrics

Types of Resilience

Physical Resilience

Environmental Redundancy

Domain Resilience

Vendor Resilience

Software Resilience

Software Versioning

In-House vs. Commercial Off-the-Shelf (COTS) Software

Resilience in the Cloud

Consequences of Authentication and Authorization Resilience

Client and Server Agent Resilience

Audit Trail Resilience

Audit Trail Reputability

Reliability of Auditable Data

Proactive Resilience Validation

Network Infrastructure Resilience Consideration

Summary

Chapter 21 Zero Trust in Industrial Manufacturing Vertical

Table of Contents

Introduction to Industrial Networking

Pillars of ZTNA for Industrial Plant Networks

Security Foundation with Firewalls

Visibility with the Network as a Sensor

Creating Granular Trust Zones Using Microsegmentation

Use Case 1

Use Case 2

Correlation and Automation to Contain Threats

Secure Remote Access with ZTNA

Extending ZTNA in a Noncarpeted Environment with Cisco SD-Access

Extended Node (EN)

Policy Extended Node (PEN)

Summary

Chapter 22 Third-Party SDN Integrations

Introduction to Third-Party SDN Integrations

End-to-End Policy Strategy in a Multivendor Environment

Benefits of End-to-End Segmentation

Challenges in Multivendor Environments

Scenario 1: Site Type A with Cisco SD-WAN Integration

Scenario 2: Site Type B with SD-WAN Integration

Scenario 3: Site Type C with SD-WAN Integration

Scenario 4: Inter-Regional Communication

Why VXLAN-EVPN?

BGP EVPN Detailed Traffic Flow and Architecture

Security Considerations in the Campus

Firewall Connectivity in the Campus

Third-Party Vendor Firewall Policy Integration

Highly Resilient Firewall Integrations

Table of Contents

Summary

References

Chapter 23 Infrastructure as Code (IaC)

Introduction

Evolution of Automation in Network Device Deployment and Management

Working with Structured Data

Revision Control

Building a Data Model

Network Controllers vs. Direct to Device

Deploying an IaC Architecture

Securing IaC Provisioning

NETCONF Service-Level Restrictions

Deploying a Resilient as Code Infrastructure

As Code Today

Transitioning to a Network as Code

Pre-Validation in the Physical Replica or a Digital Twin

Summary

Index