Digital Edge

Digital Edge – AWS

Modern Solutions for Infrastructures in AWS: *Zero Trust, Code Based Cybersecurity, and Certification in The Cloud*

By:
Michael Petrov
Founder & CEO

Digital Edge Ventures, LLC
7 Teleport Drive
Staten Island, NY 10311

Zero Trust - Access Control and Identity Management

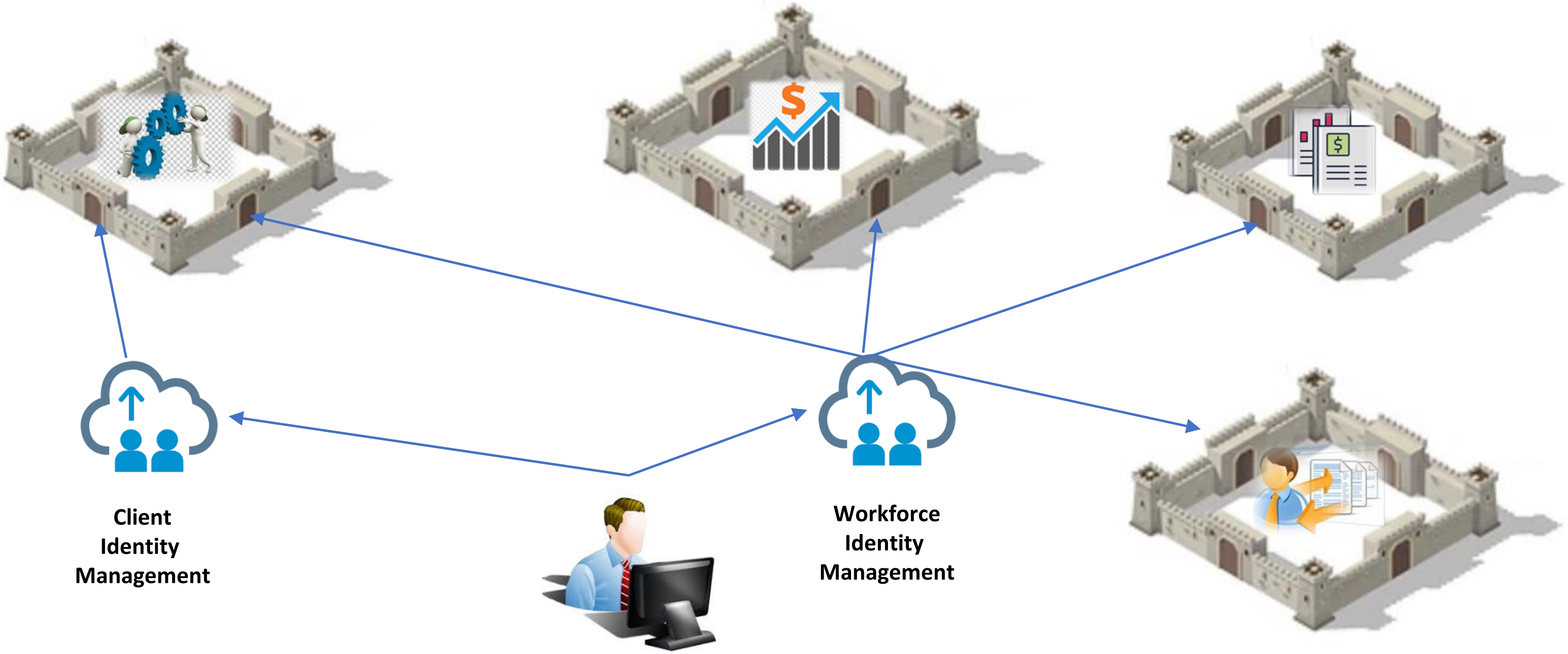
- Modernize standard perimeter-based access and identity control by implementing zero trust

- Why Zero Trust is important:
  1. *Identity and access are key to security*
  2. *Increase cloud security*
  3. *Remote workforce management*
  4. *Increased efficiency in access management*

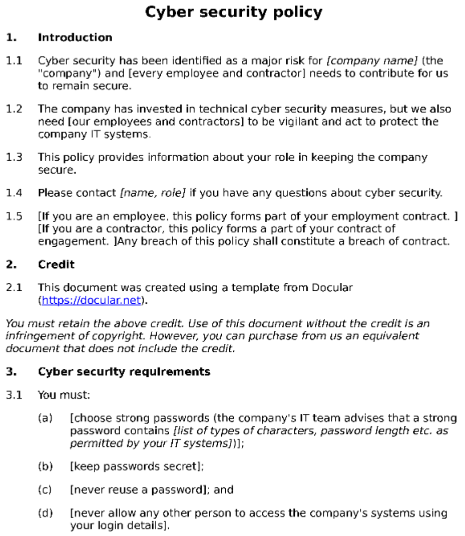
- Digital Edge’s team of strategic cybersecurity advisors and AWS certified engineers deliver compliant cybersecurity best-practices and data protection services such as zero trust and code-based cybersecurity. These services align with required laws, regulations, or frameworks for our clients’ cloud environments

Perimeter Based (Traditional) Access Control:

Information Classification Based Access Control (example):



Code Based Cybersecurity Compliance



Cyber security policy

1. Introduction

1.1 Cyber security has been identified as a major risk for *[company name]* (the "company") and [every employee and contractor] needs to contribute for us to remain secure.

1.2 The company has invested in technical cyber security measures, but we also need [our employees and contractors] to be vigilant and act to protect the company IT systems.

1.3 This policy provides information about your role in keeping the company secure.

1.4 Please contact *[name, role]* if you have any questions about cyber security.

1.5 [If you are an employee, this policy forms part of your employment contract.] [If you are a contractor, this policy forms a part of your contract of engagement.]Any breach of this policy shall constitute a breach of contract.

2. Credit

2.1 This document was created using a template from Docular (https://docular.net).

You must retain the above credit. Use of this document without the credit is an infringement of copyright. However, you can purchase from us an equivalent document that does not include the credit.

3. Cyber security requirements

3.1 You must:

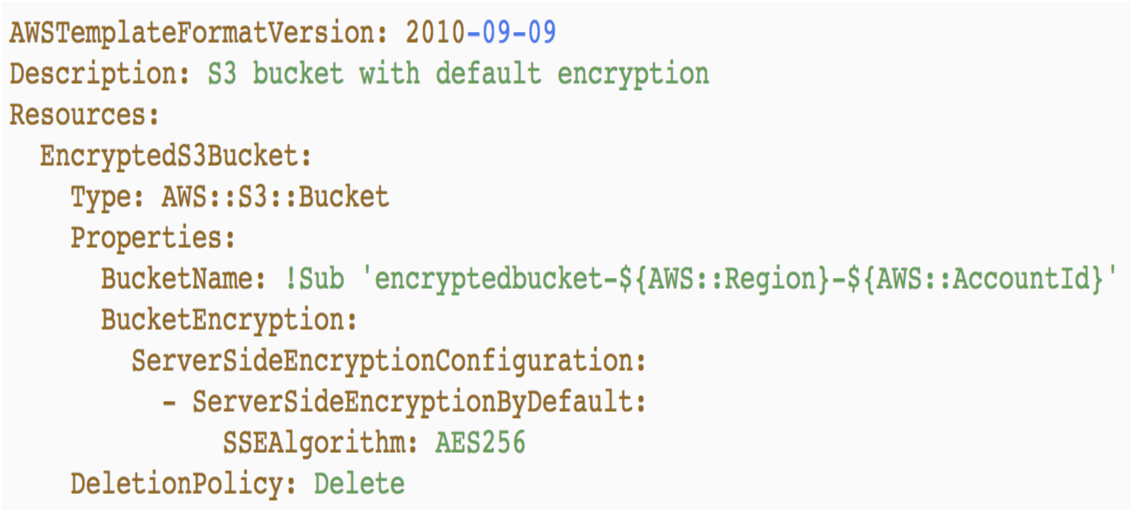
(a) [choose strong passwords (the company's IT team advises that a strong password contains *[list of types of characters, password length etc. as permitted by your IT systems]*)];

(b) [keep passwords secret];

(c) [never reuse a password]; and

(d) [never allow any other person to access the company's systems using your login details].

Security as a Document



```
AWSTemplateFormatVersion: 2010-09-09
Description: S3 bucket with default encryption
Resources:
  EncryptedS3Bucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: !Sub 'encryptedbucket-${AWS::Region}-${AWS::AccountId}'
      BucketEncryption:
        ServerSideEncryptionConfiguration:
          - ServerSideEncryptionByDefault:
              SSEAlgorithm: AES256
    DeletionPolicy: Delete
```

Security as a Code (Automated Security)

- **Security automation is the new norm:**

  Cloud environments are mostly adapted for enablement and agility, which add challenges to manageability.

- **Key questions related to cloud environment manageability:**

  1. *Who made changes?*
  2. *What was changed?*
  3. *Has the changed induced risk?*

- **Why security automation is important:**

  1. *Many of the latest cybersecurity breaches were due to misconfigurations of client environments in the cloud*
  2. *New methods detect misconfigurations in real time*
  3. *New methods better automate compliance*
  4. *New methods detect mistakes of DevOps*

Certification in the Cloud

NIST
National Institute of Standards and Technology

ISO
International Organization for Standardization

HITRUST™

SSAE 18
type 2
COMPLIANT
SOC 2
SAS 70 SSAE 16 SSAE 18

Digital Edge operates within the minimum default compliant frameworks, NIST 800 and ISO 27001. In addition, we observe and overlay all other popular frameworks or laws within our IT environment and compliance audit practices for those clients that may be subject to specific industry regulations or laws. As a result, we have successfully prepared many clients’ cloud environments to become certified or compliant with one or more frameworks or laws and/or delivered the compliant service environment needed.

- Why certification in the cloud is important:

1. *It is not simple to implement framework in public clouds.*
2. *Agility of the cloud will make hard to maintain compliance.*
3. *Organization must provide reasonable safeguards.*
4. *What is REASONABLE?*
5. *Implementations MUST adhere to a standard. Standards are not a goal but a way of operating.*

- Duty to Care:

Regulators do not require the prevention of all incidents, as frameworks do not guarantee full protection. BUT:

1. *We are responsible for implementing the necessary safeguards to prevent harm (the essence of “Duty to Care”)*
2. *Judges use “Duty to Care” to determine liabilities in data breaches*
3. *The easiest way to prove REASONABILITY is to implement a standard*

About Digital Edge

Digital Edge Ventures, Inc. (“Digital Edge”) is a 20+ year-old Managed Security Service Provider and IT consulting firm based in New York City. Digital Edge provides design, implementation, and support for Information Security and Privacy Management Systems in public clouds, including in AWS as an AWS Advanced Tier consulting partner. We help clients achieve major certifications such as ISO 27001, PCI, HITRUST, SSAE 18 SOC2, OSPAR as well as comply with major cybersecurity laws and regulations.

Digital Edge is a team of highly professional and certified subject matter experts enforced by a Security Operation and Support Organization available 24/7.