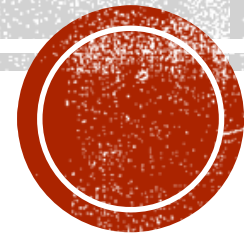


OPTIMIZED OFF-LINE RISK ASSESSMENT FRAMEWORK FOR CSPs

Ashley Painter

Joshua Haupt

Matthew Hall

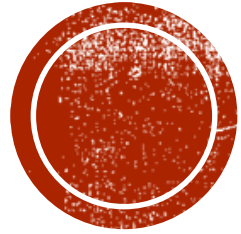


MISSION

- Choose a federation of CSPs to migrate entities of an application to
- An entity is an independent component of an application.
- Requires....
 - Security needs of Application's entities (CIA and Criticality)
 - Vendor Assessment
 - Cost-Benefit Tradeoff Analysis

Generated 24.7.2015
SLA Amazon EC2
Availability 5 - The CSP promises 99.99% up-time.
Security and Privacy 10 - (5 x 2) The CSP has Government level certification.
Performance 4 - CPU frequency is specified.
...
Total Score 39

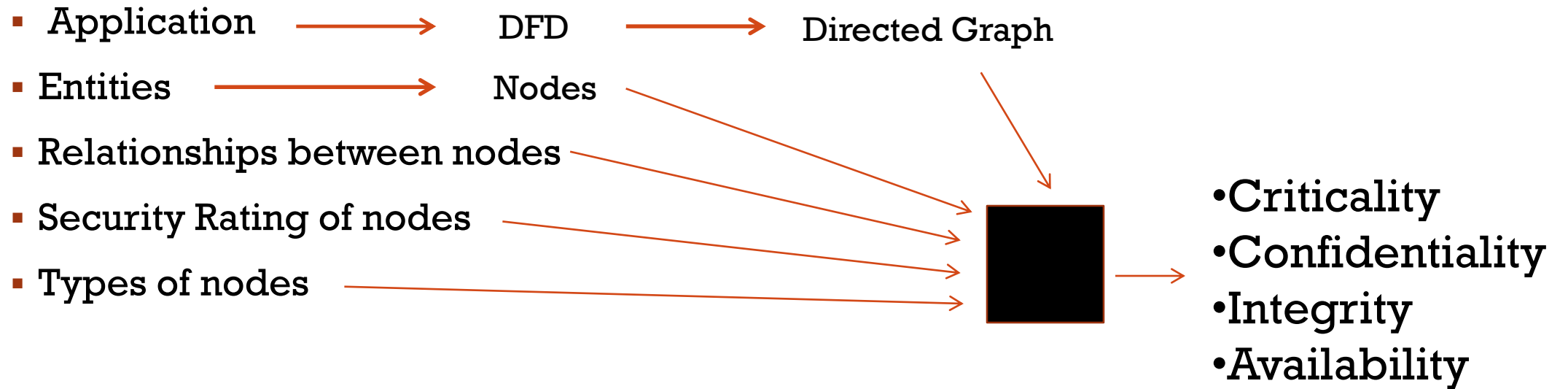




APPLICATION ASSESSMENT FRAMEWORK

Ashley Painter

FRAMEWORK



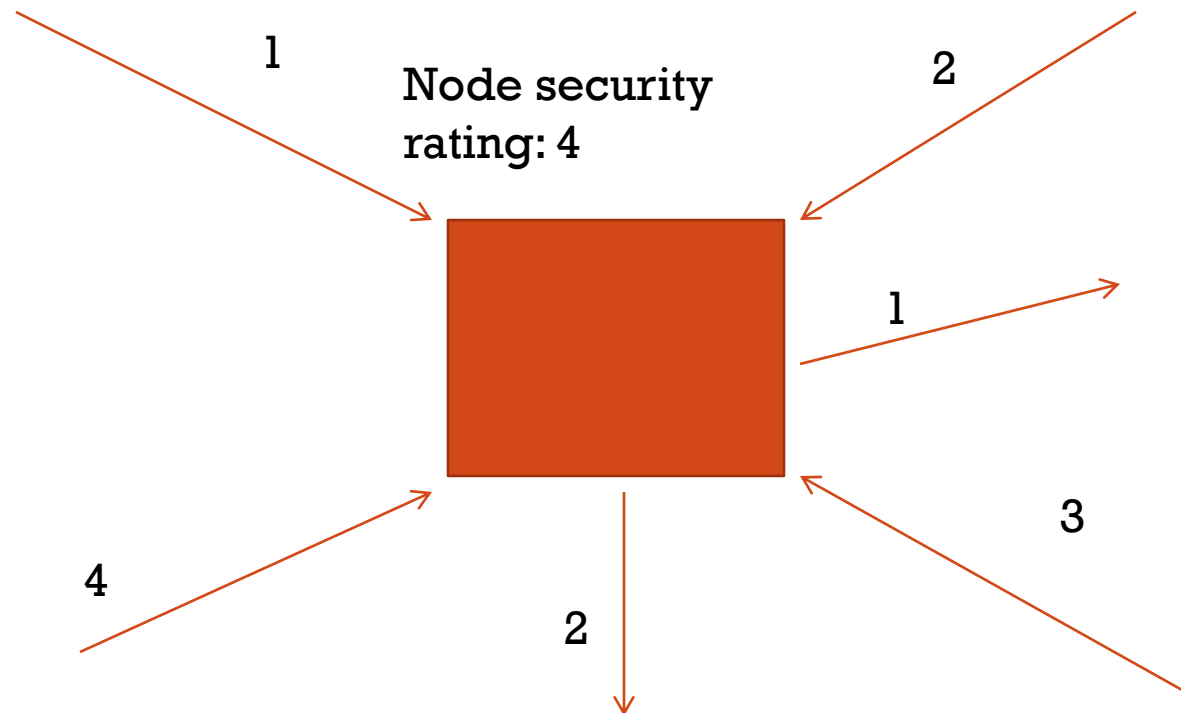
SECURITY RATING OF EACH EDGE

- (Low = 1) The lowest rating. Data which needs to be available but if leaked it will cause minimal damage, may already be available on the internet
- (Medium = 2) For low value personal information: addresses, names, other business information with approximately equal amount of potential damage if leaked
- (High = 3) Personal information: Social Security Numbers, Bank account information, business information with approximately equal amount of potential damage
- (Extreme = 4) Information that is highly sensitive for which leakage of, damage to, or modification of could cause company failure or severe injury to employees or customers.



SECURITY RATING OF NODES

- The highest security rating of the edges that connect to that node



NODE TYPES

{Alpha}

- Representing an entity that stores either highly confidential data or logging data

{Beta}

- Interacts with users of the application
- have a high need for accessibility
- API's, user interfaces, direct to user screen movie streaming
- Anything that takes data directly from a user OR outputs data to them in any format



NODE TYPES CONTINUED

{Gamma}

- Does work on data or directs it to other
- A process that does not fall under any other type

{Delta}

- Outside of the application's control
- Has unique challenges because examples range from banks to websites to other applications which may or may not have adequate security measures and are unlikely to divulge them if they do

{Epsilon}

- Stores data but does not fall under the Alpha type.



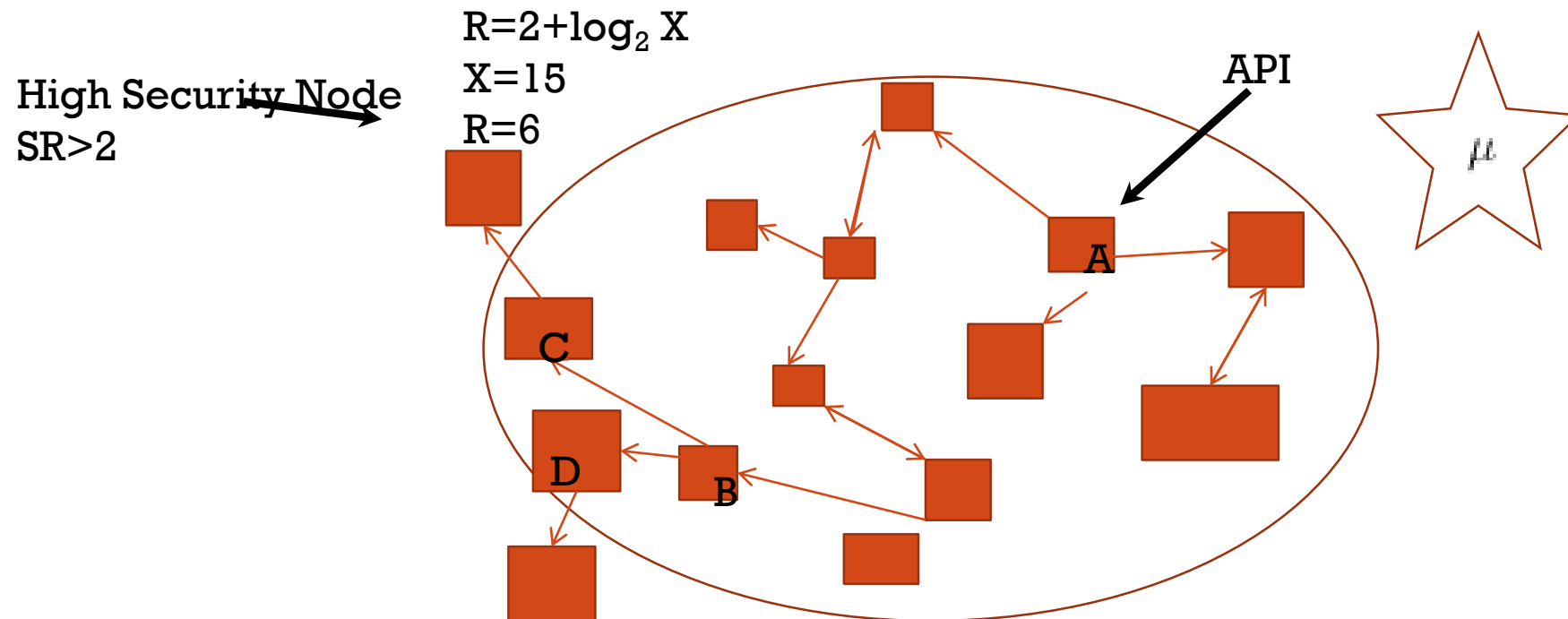
NODE ADJUSTMENT FOR TYPE

- I_v = Initial value for type of node
 - changes based off of which attribute of which node is being analyzed
 - This is where the individual security needs of a node are taken into account
- Cr = the value of I_v when evaluating Criticality for an individual node
- C = the value of I_v when evaluating Confidentiality for an individual node
- I = the value of I_v when evaluating Integrity for an individual node
- A = the value of I_v when evaluating Availability for an individual node
 - Alpha Cr=2 C=2 I=2 A=0
 - Beta Cr=1 C=0 I=0 A=2
 - Gamma Cr=0 C=0 I=2 A=0
 - Delta Cr=0 C=0 I=0 A=0
 - Epsilon Cr=0 C=1 I=1 A=0



GLOBAL AREA

- Only one case that the global connections matter that of a high A node with connections over many edges to a high security node.



USER INPUT

- Nodes
- Type of each node
- Edges
- Security level of each edge



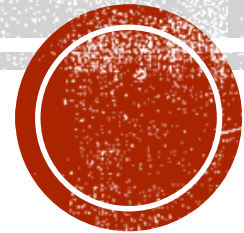
Algorithms for analyzing each node in a single direction

$$\textit{Confidentiality} = I_v + 1/M + \textit{Flow}() \quad (1)$$

$$\textit{Availability} = I_v + M + \textit{Flow}() \quad (2)$$

$$\textit{Integrity} = I_v + 1/M + M + \textit{Flow}() \quad (3)$$

$$\textit{Criticality} = I_v + v + \mu \quad (4)$$



OUTPUT FOR EACH NODE

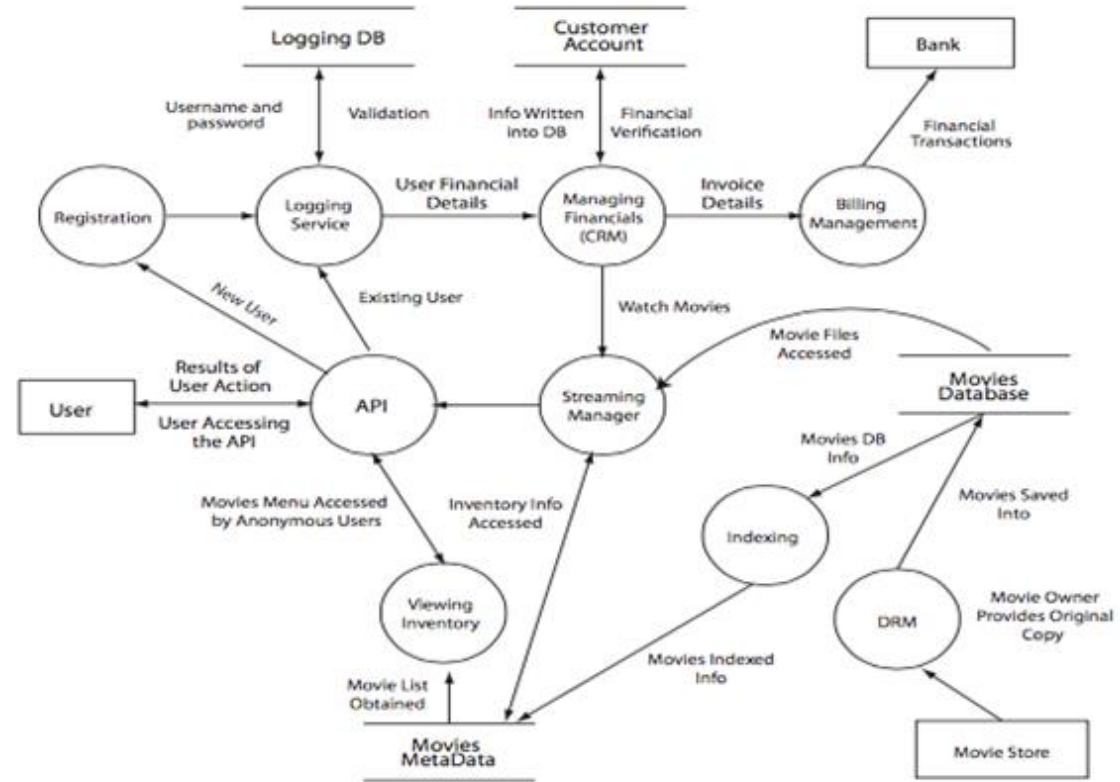
- Confidentiality: in
- Integrity: in
- Availability: in
- Criticality: in



- Confidentiality: out
- Integrity: out
- Availability: out
- Criticality: out



EXAMPLE



Sen, Amartya, and Sanjay Madria. "Off-line risk assessment of cloud service provider." *Services (SERVICES), 2014 IEEE World Congress on. IEEE, 2014.*



EXAMPLE CONTINUED

Bank

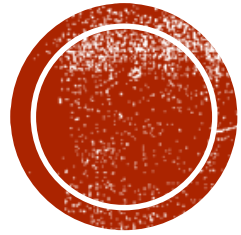
9.4 Output

Example of the output for the entity bank

9.4.1 Bank

	Criticality	Confidentiality	Integrity	Availability
In	3	2.33	5.33	4
Out	3	4.33	7.33	6





CLOUD VENDOR ASSESSMENT MODEL

Joshua Haupt

SLA GRADING FRAMEWORK

- Autonomous approach to remove possible human bias
- 8 Categories
 - Availability
 - Compensation
 - Scalability
 - Security and Privacy
 - Performance
 - Understanding of Costs
 - Ease of Configuration
 - Compatibility



AVAILABILITY

- The assurance that an enterprise IT infrastructure has suitable recoverability and protection from system failures, natural disasters or malicious attacks (Gartner).
- Point system
 - 0 the word availability or a synonym of it is **not** present.
 - 1 the word availability or a synonym of it **is** present.
 - 2 the promised uptime is between 99.00% and 99.50%.
 - 3 the promised uptime is between 99.50% and 99.80%.
 - 4 the promised uptime is between 99.80% but less than 99.99%.
 - 5 the promised uptime is 99.99%.



COMPENSATION

- The reimbursement promised by a cloud vendor in the event the vendor fails to uphold to its SLA.
- Points
 - 0 the phrase SLA compensation or a similar one is not present.
 - 1 the phrase SLA compensation or a similar one is present.
 - 3 the SLA will compensate credit with the user providing evidence of downtime.
 - 5 the SLA states that compensation will be given automatically if the CSP notices downtime.



SCALABILITY

- The measure of a systems ability to increase or decrease in performance and cost in response to changes in application and system processing demands (Gartner)
- Points
 - 0 Scalability or a synonym is not present
 - 1 Scalability or a synonym is present
 - 2 Scaling up is possible
 - 3 Scaling down is possible
 - 4 Auto-scaling is possible
 - 5 Auto-scaling is possible within client's budget constraints and available resources are displayed to the client



SECURITY AND PRIVACY

- How well the CSP protects the user's private data.
 - What security features have been implemented and what certifications the CSP has
 - Security and Privacy carry a weight factor of two
 - It is considered the largest risk clients face when migrating to a cloud service platform (Offline Risk Assessment).
- Points
 - 0 Security, privacy or any related words are not present.
 - 1 Security, privacy or any related words are present.
 - 2 At least one security feature implemented.
 - Ex. VPN, Disk Encryption, individual OS kernels.
 - 3 Two or more security features implemented and supports Federated Identity Management
 - Ex. External authentication server
 - 4 Financial, PCI, certification.
 - 5 High level, health-care or Gov, certification.



PERFORMANCE

- The capabilities of a service offered by a cloud service provider which are observed under particular conditions
- Points
 - 0 Nothing is mentioned regarding performance
 - 1 Guarantees, or promises are made
 - 2 CPU core count, disk space or storage, network transfer, bandwidth and memory are specified
 - 3 HDD or SSD usage is specified
 - 4 CPU frequency is specified
 - 5 Disk IO and/or response time is specified



UNDERSTANDING OF COSTS

- How the costs for the service and various add on services is presented.
 - Are they presented in a way that is easy for anybody to understand?
- Points
 - 0 Nothing is mentioned
 - 1 Costs are listed as per specified unit
 - 2 A calculator is provided to calculate costs per resource
 - 3 The ability to implement a budget or spending limit is in place
 - 4 Packages or plans are provided
 - 5 Managed support is provided to help the client understand costs



EASE OF CONFIGURATION

- How easy it is for a client to set up and utilize a CSPs platform.
- Points
 - 0 Nothing is mentioned.
 - 1 The word easy or a synonym of it is mentioned.
 - 2 There is documentation.
 - 3 Click to install is available.
 - 4 A support number is provided.
 - 5 Managed service is available.



COMPATIBILITY

- How well the cloud service platform can be integrated with other cloud service provider's platforms
- How well data can be exported from one CSP to another in the event a client wishes to migrate to another CSP



COMPATIBILITY

- **Score**
 - 0 Proprietary APIs are used and no emulation is available. Data is not easily exportable.
 - 1 Proprietary APIs are used and some emulation is available. Data is easily exportable in a proprietary format.
 - 2 Proprietary APIs are present but decent emulation is available and data is easily exportable in a non proprietary format.
 - For example many CSPs have implemented support for applications that use Amazon's S3 API.
 - 4 Open source APIs are used but data is not easily exportable.
 - 5 The provider uses an open source platform APIs and allows easy exporting of data in a common format that can be easily uploaded to another CSP.



EXAMPLE OUTPUT

Generated 23.5.2015

SLA Amazon EC2

Category

Availability 5 - The CSP promises 99.99% up-time.

Compensation 3 - The CSP will compensate credit for downtime if the client contacts them with evidence.

Scalability 5 - Auto scaling is possible within client's budget constraints and available resources are displayed to the client.

Security and Privacy 10 - (5 x 2) - The CSP has Government level certification.

Performance 4 - CPU frequency is specified.

Understanding of Costs 5 - Managed support is available to help the client understand costs.

Ease of configuration 5 - Managed support is available to help the client set up.

Compatibility 2 - Proprietary APIs are used but other CSPs have implemented decent emulation of the APIs.

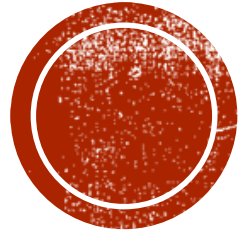
Total Score 39



SOURCES

- Madria, Sanjay, and Amartya Sen. "Offline Risk Assessment of Cloud Service Providers." *Cloud Computing, IEEE 2.3* (2015): 50-57.
- Alhamad, Mohammed, Tharam Dillon, and Elizabeth Chang. "Conceptual SLA framework for cloud computing." *Digital Ecosystems and Technologies (DEST)*, 2010 4th IEEE International Conference on. IEEE, 2010.





COST-BENEFIT TRADE OFF WITH RESPECT TO SECURITY COVERAGE ON CSPs

Matthew Henry Hall

RELATION TO VENDOR ASSESSMENT



http://d1u2s20mo6at4b.cloudfront.net/wp-content/uploads/choose_wisely.png

- Vendor Assessment chooses which CSPs have promised services that suit an application's needs
- Cost Benefit Trade Off Analysis will reinforce those results presented



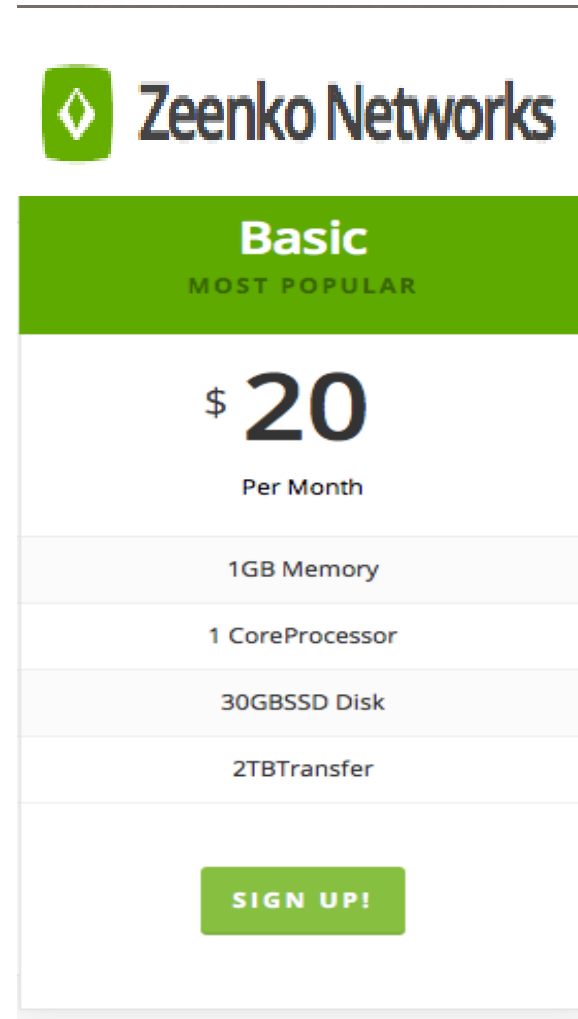
MOTIVATION FOR COST – BENEFIT TRADE OFF

- Migrating to a CSP can save money for whomever chooses a smart way to move the parts of their application
- Different CSPs are better suited to the needs of different entities
- Finding a federation of CSPs for an application will cut costs in
 - Electricity
 - Price for Securing Infrastructure
 - Hardware, Storage rent, and more...



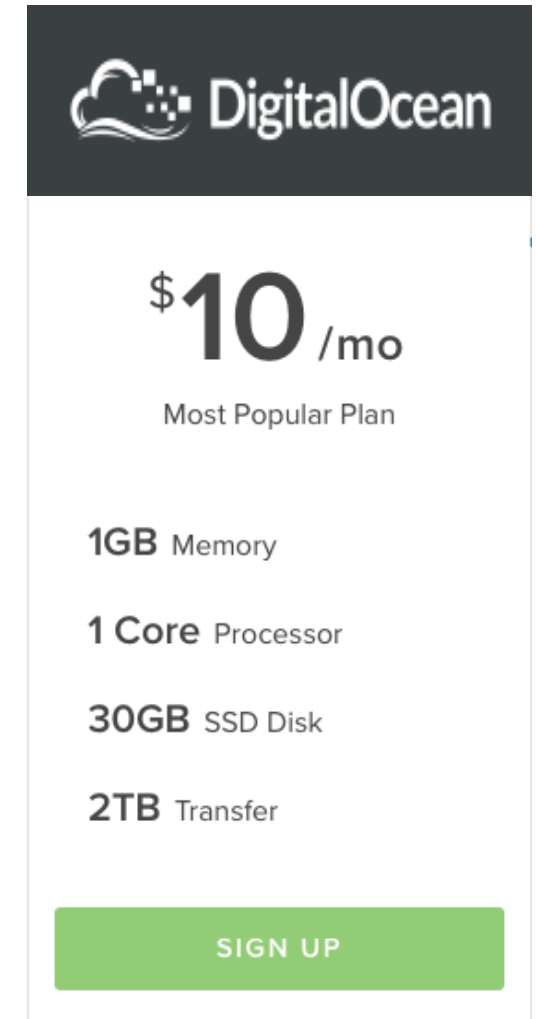
CONTEXT

- Raw cost in dollars alone is misleading unless you can measure what a difference in prices earns you
- Zeenko Networks and Digital Ocean present the same services, but Digital Ocean is half the price
- Which CSP will you choose?



The screenshot shows the Zeenko Networks website. At the top is the Zeenko Networks logo. Below it is a green banner with the text "Basic" and "MOST POPULAR" in white. The main pricing information is displayed in a large font: "\$ 20 Per Month". Below this, the specifications for the plan are listed in a table-like format: "1GB Memory", "1 CoreProcessor", "30GBSSD Disk", and "2TBTransfer". At the bottom of the page is a green button with the text "SIGN UP!" in white.

<https://zeenko.com/cloud-services/public-cloud-servers/#>



The screenshot shows the DigitalOcean website. At the top is the DigitalOcean logo. Below it is a dark grey banner with the text "DigitalOcean" in white. The main pricing information is displayed in a large font: "\$ 10 /mo" and "Most Popular Plan". Below this, the specifications for the plan are listed: "1GB Memory", "1 Core Processor", "30GB SSD Disk", and "2TB Transfer". At the bottom of the page is a green button with the text "SIGN UP" in white.

<https://www.digitalocean.com/pricing/>



FRAMEWORK FOR MAKING AN INFORMED MIGRATION DECISION

- Must know
 - Price of hosting the entities of an application yourself
 - Price of hosting them on different clouds
 - Security weaknesses in your entities
 - Weaknesses that arise from moving to a CSP





TRADE-OFF STEP BY STEP

- Step One – Cost Difference Metric
 - Find the difference between hosting an entity yourself for one year and having the cloud host it for the same time
- Step Two – Scoring Weaknesses
 - Find and Score the weaknesses from CWE that that entity will have when moving to a CSP
 - Scoring is based on the weakness attributes presented earlier.
- Step Three – Tallying Scores
 - Find the sum of the weakness scores (Total) for an entity and the sum of the weakness scores covered by a CSP (WC)
 - Score of Weaknesses Uncovered (WU) is Total minus Weaknesses Covered ... $WU = Total - WC$
- Step Four – Security Difference Metric
 - Compute Weaknesses Covered minus Weaknesses Uncovered for chosen clouds
 - Final Score = $WC - WU$



TRADE-OFF FINAL STEPS

- Step Five – Combining Cost and Security
 - Standardize both difference metrics with respect to the entity being analyzed
 - Add the standardized results together
- Step Six – Should it Stay or Should it Go?
 - Find the cloud whose sum from the previous result is greatest
 - If that CSP have a positive Cost Difference and Security Difference then present that cloud for migration
 - Else host locally

