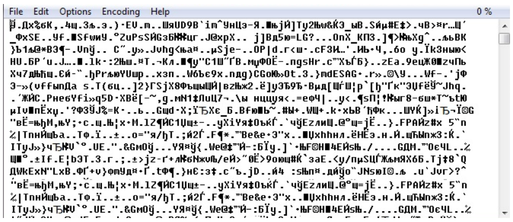
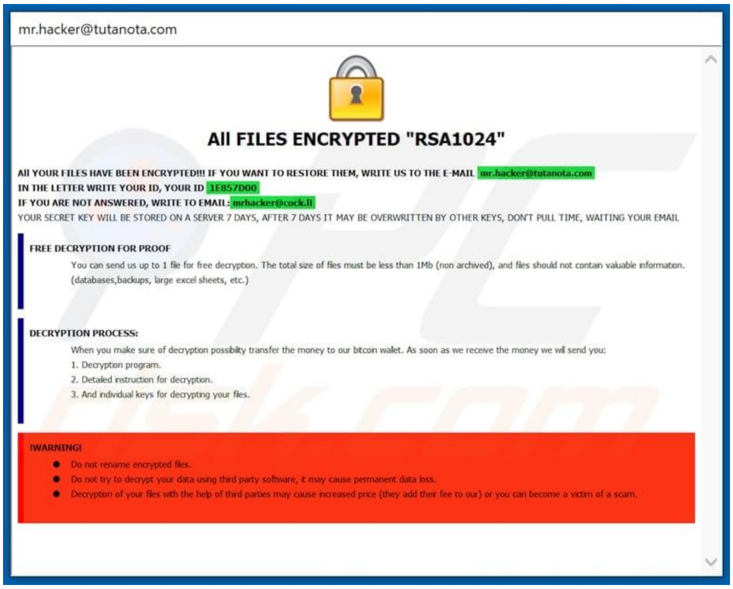
Benefits Of Moving to Cloud Based Technology

Kevin Nye
Regional Account Manager
Software Solutions, Inc.

1





mr.hacker@tutanota.com

All FILES ENCRYPTED "RSA1024"

All YOUR FILES HAVE BEEN ENCRYPTED!!! IF YOU WANT TO RESTORE THEM, WRITE US TO THE E-MAIL mr.hacker@tutanota.com
IN THE LETTER WRITE YOUR ID, YOUR ID 1E857D00
IF YOU ARE NOT ANSWERED, WRITE TO EMAIL: mrhacker@cock.li
YOUR SECRET KEY WILL BE STORED ON A SERVER 7 DAYS, AFTER 7 DAYS IT MAY BE OVERWRITTEN BY OTHER KEYS, DON'T PULL TIME, WAITING YOUR EMAIL

FREE DECRYPTION FOR PROOF

You can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

DECRYPTION PROCESS:

When you make sure of decryption possibility transfer the money to our bitcoin wallet. As soon as we receive the money we will send you:

1. Decryption program.
2. Detailed instruction for decryption.
3. And individual keys for decrypting your files.

!WARNING!

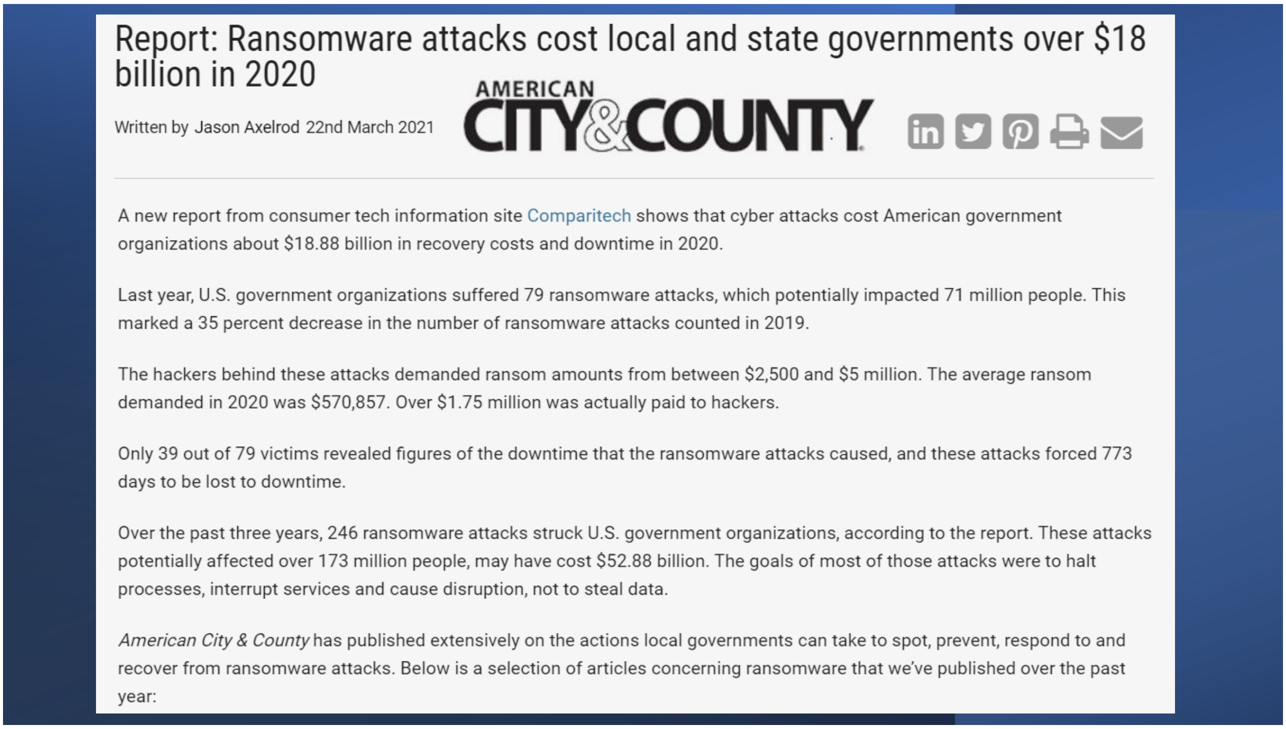
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

2

Ransom: $570,857

Source: American City & County

3



Report: Ransomware attacks cost local and state governments over $18 billion in 2020

Written by Jason Axelrod 22nd March 2021

AMERICAN CITY&COUNTY

A new report from consumer tech information site Comparitech shows that cyber attacks cost American government organizations about $18.88 billion in recovery costs and downtime in 2020.

Last year, U.S. government organizations suffered 79 ransomware attacks, which potentially impacted 71 million people. This marked a 35 percent decrease in the number of ransomware attacks counted in 2019.

The hackers behind these attacks demanded ransom amounts from between $2,500 and $5 million. The average ransom demanded in 2020 was $570,857. Over $1.75 million was actually paid to hackers.

Only 39 out of 79 victims revealed figures of the downtime that the ransomware attacks caused, and these attacks forced 773 days to be lost to downtime.

Over the past three years, 246 ransomware attacks struck U.S. government organizations, according to the report. These attacks potentially affected over 173 million people, may have cost $52.88 billion. The goals of most of those attacks were to halt processes, interrupt services and cause disruption, not to steal data.

American City & County has published extensively on the actions local governments can take to spot, prevent, respond to and recover from ransomware attacks. Below is a selection of articles concerning ransomware that we've published over the past year:

4

Cost state and local gov’t over $18 billion

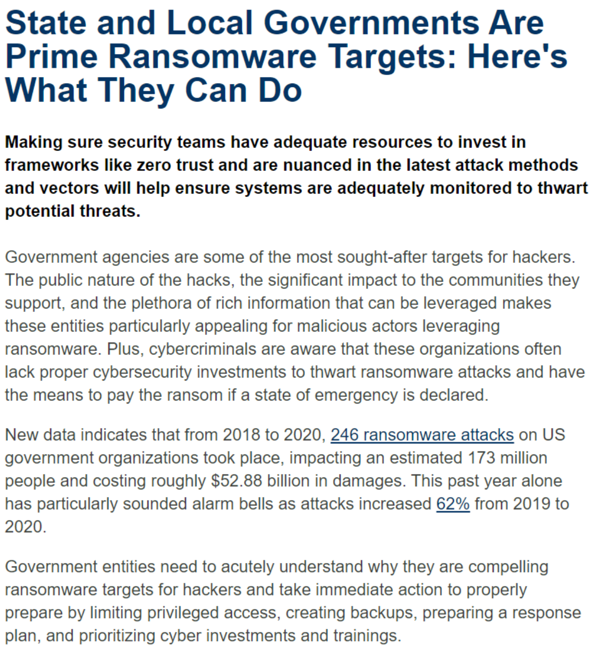
2020 average ransom = $570,857

Over $1.75 million was paid to hackers

Attacks forced 773 days downtime

Goal of attacks is to interrupt services

5



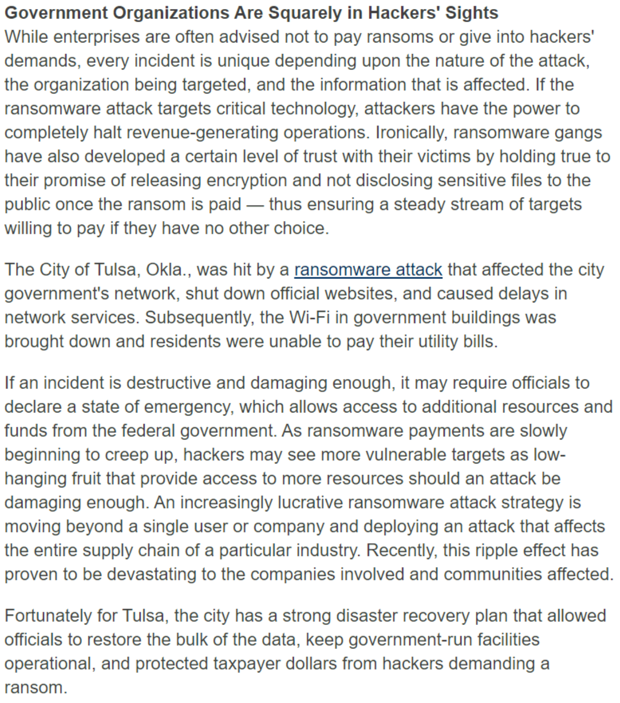
State and Local Governments Are Prime Ransomware Targets: Here's What They Can Do

Making sure security teams have adequate resources to invest in frameworks like zero trust and are nuanced in the latest attack methods and vectors will help ensure systems are adequately monitored to thwart potential threats.

Government agencies are some of the most sought-after targets for hackers. The public nature of the hacks, the significant impact to the communities they support, and the plethora of rich information that can be leveraged makes these entities particularly appealing for malicious actors leveraging ransomware. Plus, cybercriminals are aware that these organizations often lack proper cybersecurity investments to thwart ransomware attacks and have the means to pay the ransom if a state of emergency is declared.

New data indicates that from 2018 to 2020, 246 ransomware attacks on US government organizations took place, impacting an estimated 173 million people and costing roughly $52.88 billion in damages. This past year alone has particularly sounded alarm bells as attacks increased 62% from 2019 to 2020.

Government entities need to acutely understand why they are compelling ransomware targets for hackers and take immediate action to properly prepare by limiting privileged access, creating backups, preparing a response plan, and prioritizing cyber investments and trainings.



Government Organizations Are Squarely in Hackers' Sights

While enterprises are often advised not to pay ransoms or give into hackers' demands, every incident is unique depending upon the nature of the attack, the organization being targeted, and the information that is affected. If the ransomware attack targets critical technology, attackers have the power to completely halt revenue-generating operations. Ironically, ransomware gangs have also developed a certain level of trust with their victims by holding true to their promise of releasing encryption and not disclosing sensitive files to the public once the ransom is paid — thus ensuring a steady stream of targets willing to pay if they have no other choice.

The City of Tulsa, Okla., was hit by a ransomware attack that affected the city government's network, shut down official websites, and caused delays in network services. Subsequently, the Wi-Fi in government buildings was brought down and residents were unable to pay their utility bills.

If an incident is destructive and damaging enough, it may require officials to declare a state of emergency, which allows access to additional resources and funds from the federal government. As ransomware payments are slowly beginning to creep up, hackers may see more vulnerable targets as low-hanging fruit that provide access to more resources should an attack be damaging enough. An increasingly lucrative ransomware attack strategy is moving beyond a single user or company and deploying an attack that affects the entire supply chain of a particular industry. Recently, this ripple effect has proven to be devastating to the companies involved and communities affected.

Fortunately for Tulsa, the city has a strong disaster recovery plan that allowed officials to restore the bulk of the data, keep government-run facilities operational, and protected taxpayer dollars from hackers demanding a ransom.

Source: DARKReading, Tulsa World

6

From 2018 to 2020, 246 ransomware attacks on US government organizations

Attacks increased 62% from 2019 to 2020

Importance of a disaster recovery plan (backups)

7

On Premise

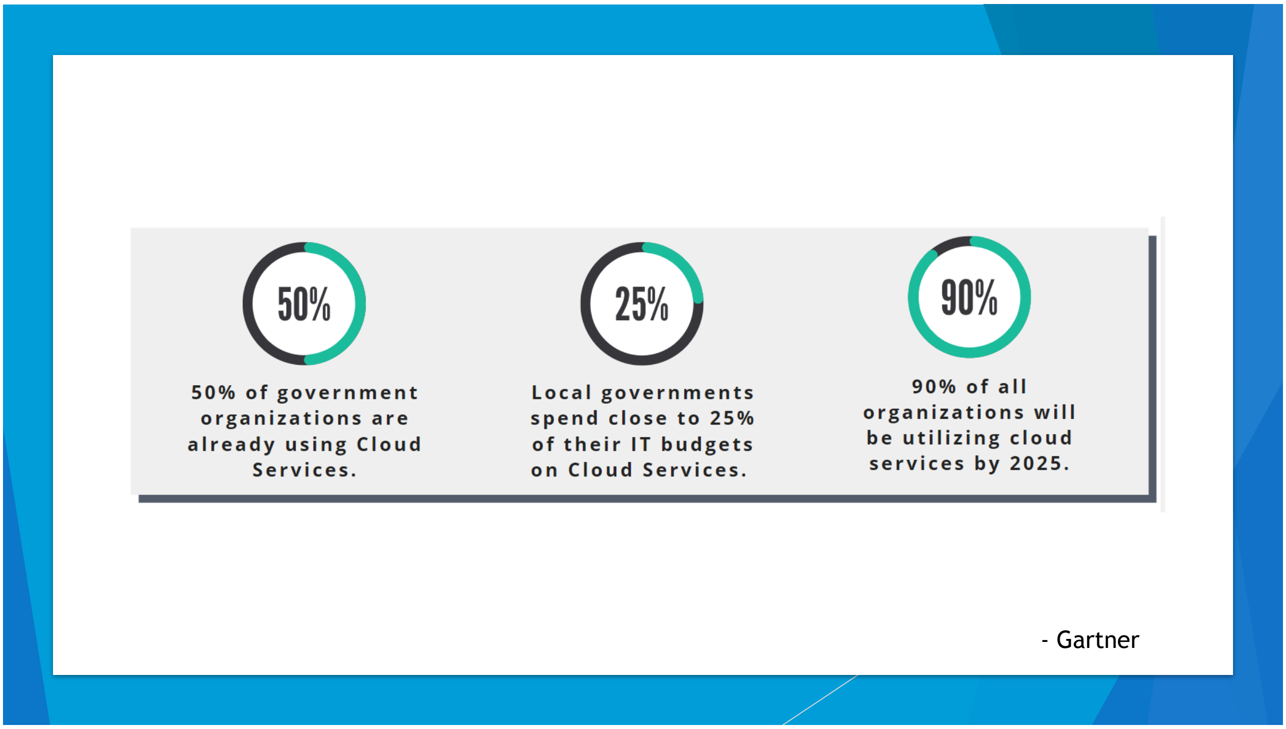
(2020). [Image]. Retrieved from https://www.stitchdata.com/resources/compare-on-premises-and-cloud-data-warehouse/

8

- Purchase and Maintain Server
- Purchase and Maintain Server Software
- Purchase and Maintain Virus Protection
- Purchase and Maintain Remote Access Connections
- Daily Backups

(2020). [Image]. Retrieved from https://www.stitchdata.com/resources/compare-on-premises-and-cloud-data-warehouse/

What is the Cloud?



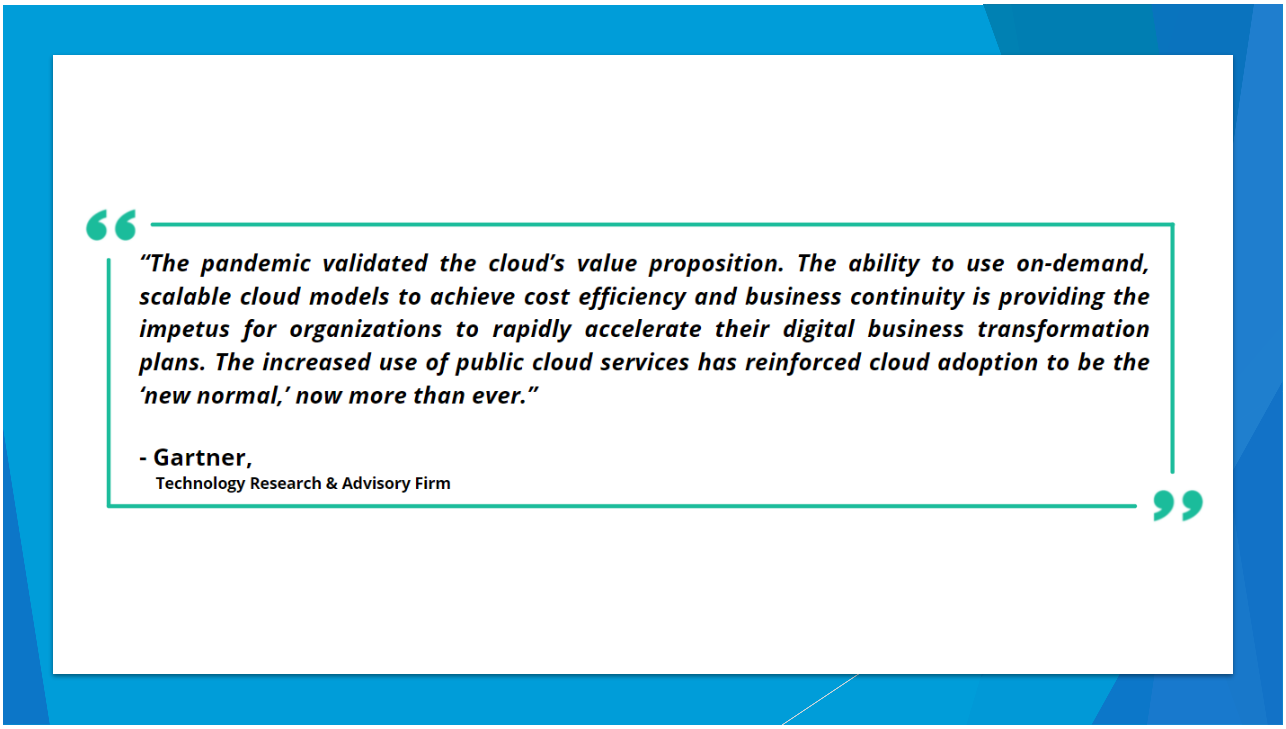
50% of government organizations are already using Cloud Services.

Local governments spend close to 25% of their IT budgets on Cloud Services.

90% of all organizations will be utilizing cloud services by 2025.

- Gartner

11



> *"The pandemic validated the cloud's value proposition. The ability to use on-demand, scalable cloud models to achieve cost efficiency and business continuity is providing the impetus for organizations to rapidly accelerate their digital business transformation plans. The increased use of public cloud services has reinforced cloud adoption to be the 'new normal,' now more than ever."*
>
> **- Gartner,**
> Technology Research & Advisory Firm

12

Software as a Service (SaaS)

- Software made available over the internet as a service
- Single-Tenant SaaS architecture

- Accessible from anywhere
- Reduce IT costs
- Increased Security
- Business Continuity
- Automated backups
- Automated updates
- Improved Support
- Scalability
- Reliable performance

Benefits

Accessible from Anywhere

15

Disclaimer: Internet Connection Still Required

16

Accessible from Anywhere

- Increase remote access capabilities and accommodate alternative work schedules and arrangements

17

Accessible from Anywhere

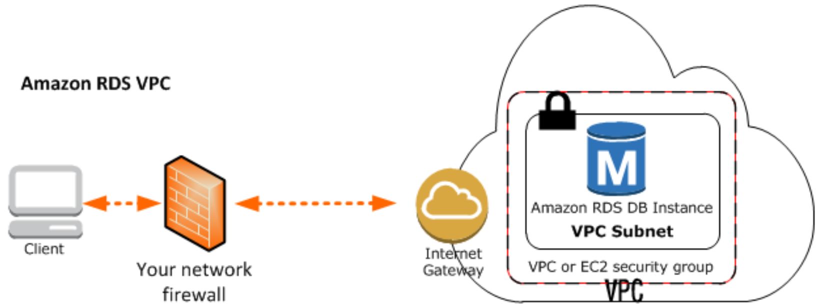
I THINK THE CLOUD'S GREAT! IT ALLOWS ME TO WORK FROM HOME. MY WIFE'S NOT SO KEEN ON IT THOUGH.
© D.Fletcher for CloudTwr

https://www.pinterest.com/virtualtechguru/cloud-comics/

18

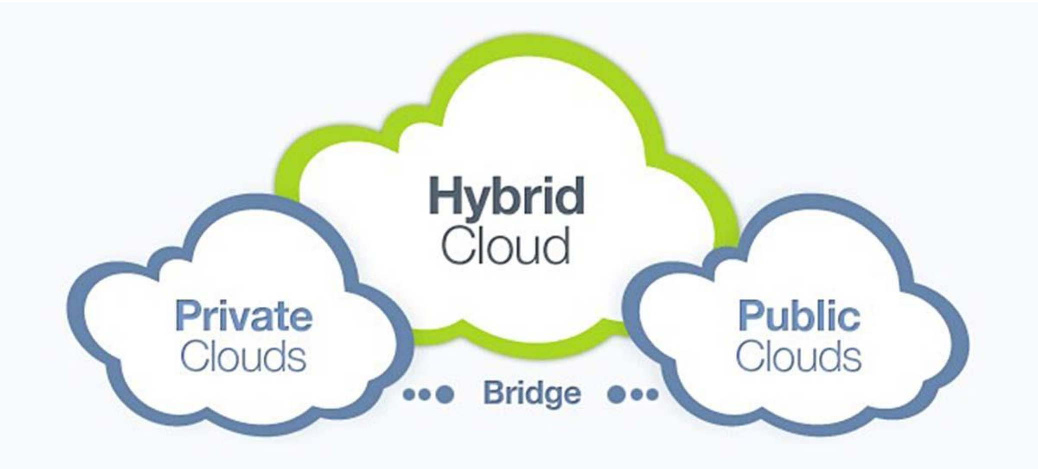
Accessible from Anywhere

- Virtual Private Cloud (VPC) allows control of network configuration, offering several layers of security controls, and the ability to allow and deny specific internet and internal traffic



https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.html

19



https://www.amyma.lu/hybrid-cloud.html

20

Reduce IT Costs

Reduce IT Costs

- Shift from upfront capital costs to operational expense
- Software and hardware fixed expenses, such as the physical server are eliminated when moving to the cloud.
  - Eliminate large IT projects
  - Eliminate the 3 to 5-year expense of purchasing a server
- More affordable total cost of ownership

Reduce IT Costs

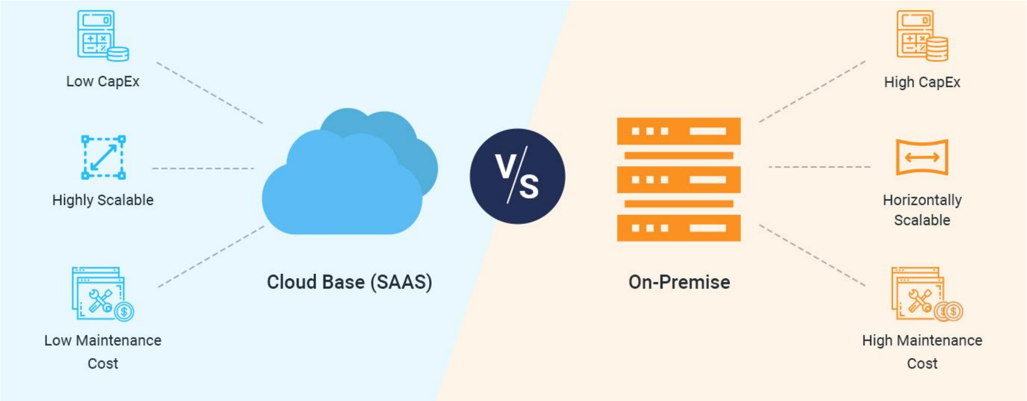
- Near-zero Maintenance, as a Service
- You are no longer responsible for supporting the IT infrastructure
  - Managed servers are kept up on the latest technology (e.g. SQL, .Net)
  - Automatic backups may be included
  - Automatic updates may be included
- Lower IT overhead costs through reduced workloads
  - Allow IT Staff to concentrate on other projects

23

Reduce IT Costs

- Performance and Scale through Provisioning
  - Pay for the actual resources needed versus paying for maximum capacity scenarios
  - Increase hardware requirements only when needed.

24



Low CapEx

Highly Scalable

Low Maintenance Cost

Cloud Base (SAAS)

V/S

On-Premise

High CapEx

Horizontally Scalable

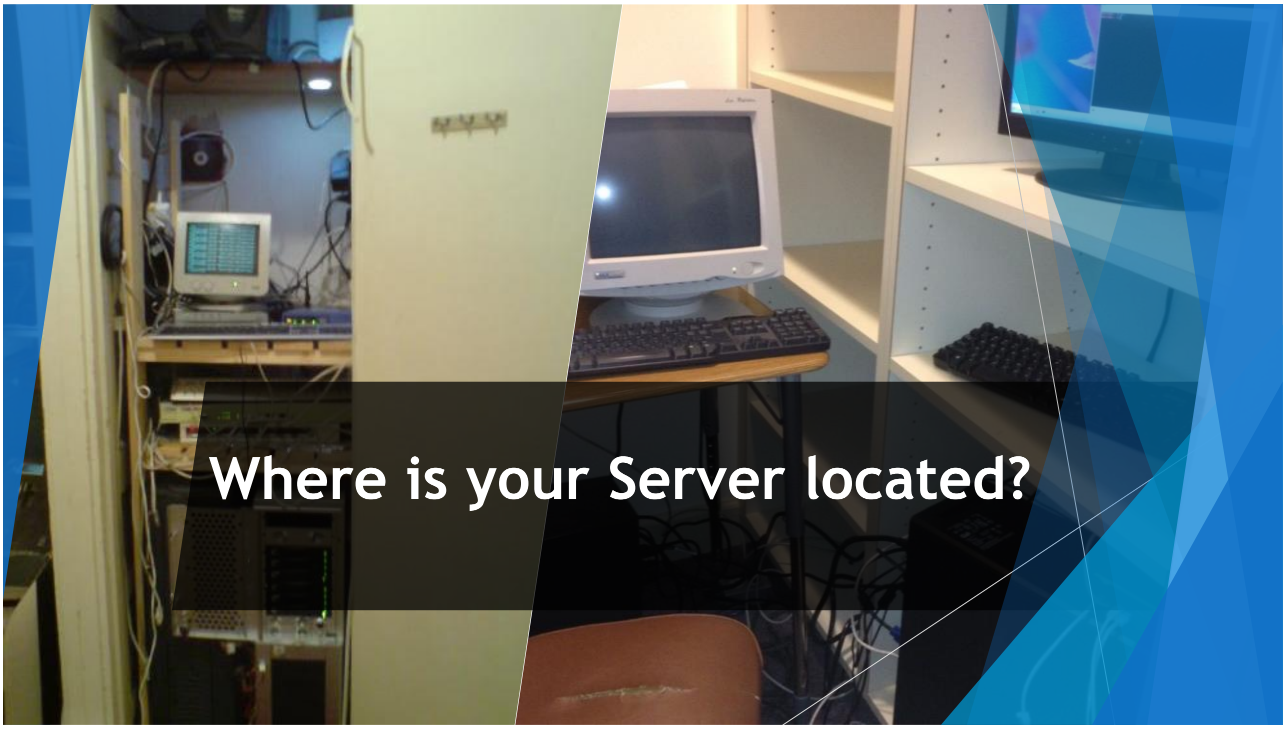
High Maintenance Cost

(2020). [Image]. Retrieved from https://www.muvi.com/blogs/cloud-video-encoding-vs-on-premise.html

25

Increased Security

26



Where is your Server located?

27

Increased Security

- Firewalls, encryption in transit, private dedicated connections, and distributed denial of service (DDoS) protection
- Intelligent threat detection and monitoring malicious activity and unauthorized behavior to protect accounts, workloads, and data

28

Increased Security

- Make sure of compliance certifications, including SOC, ISO, HIPAA, AICPA

Increased Security

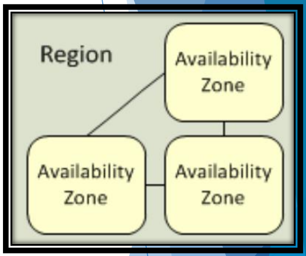
Perform penetration tests to gauge the resiliency of the application to various attacks launched against both authenticated and unauthenticated.

Business Continuity

31

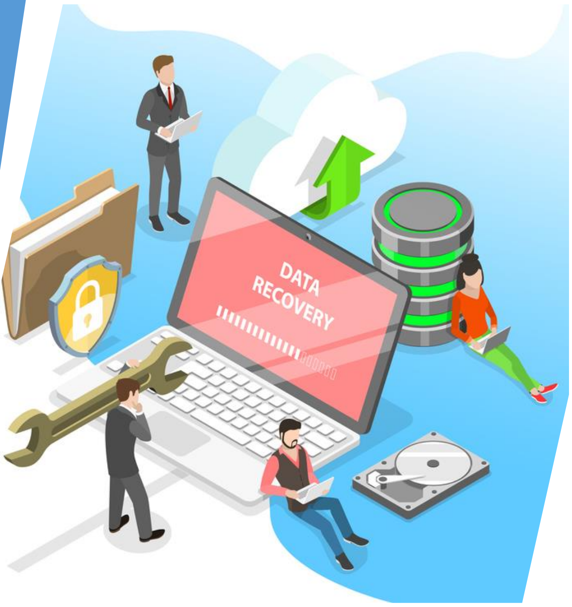
Business Continuity

- Collection of separate data centers with independent power resources, backup generators, and connectivity.
- Different grids from utility and power companies.
- If one database instance fails, then another availability zone can then handle requests



https://cloudacademy.com/blog/aws-regions-and-availability-zones-the-simplest-explanation-you-will-ever-find-around/

32



Automated Backups

33

Why Automated Cloud Backups are so important

- Local backups
  - often overwritten, lost, damaged, or not redundant.
  - go untested.
  - vulnerable to significant data loss

34

Automated Cloud Backups

- Backups can be accessed at any time as an insurance policy to recover data
- Automated backups
- Cloud Backup service is available for on premise servers

OH! THAT'S JAMERSON. HE WAS ATTEMPTING TO RECOVER DATA FROM AN ANGRY CLOUD SERVICE.
ZZZT!
ZZZT!
AL JOHNSON JR.
©CloudTweak

Automated Updates

Automated Updates

- Upgrades and enhancements can be scheduled in advance
- Reduce overhead by eliminating in house software updates

37

Improved Support

38

Improved Support

- Near-zero Maintenance, as a Service!
  - You are no longer responsible for supporting the IT infrastructure
  - Transfer responsibility to your cloud provider
- **You still own your data**
- Cloud is simply a mechanism to make accessing the software easier and more accessible

39

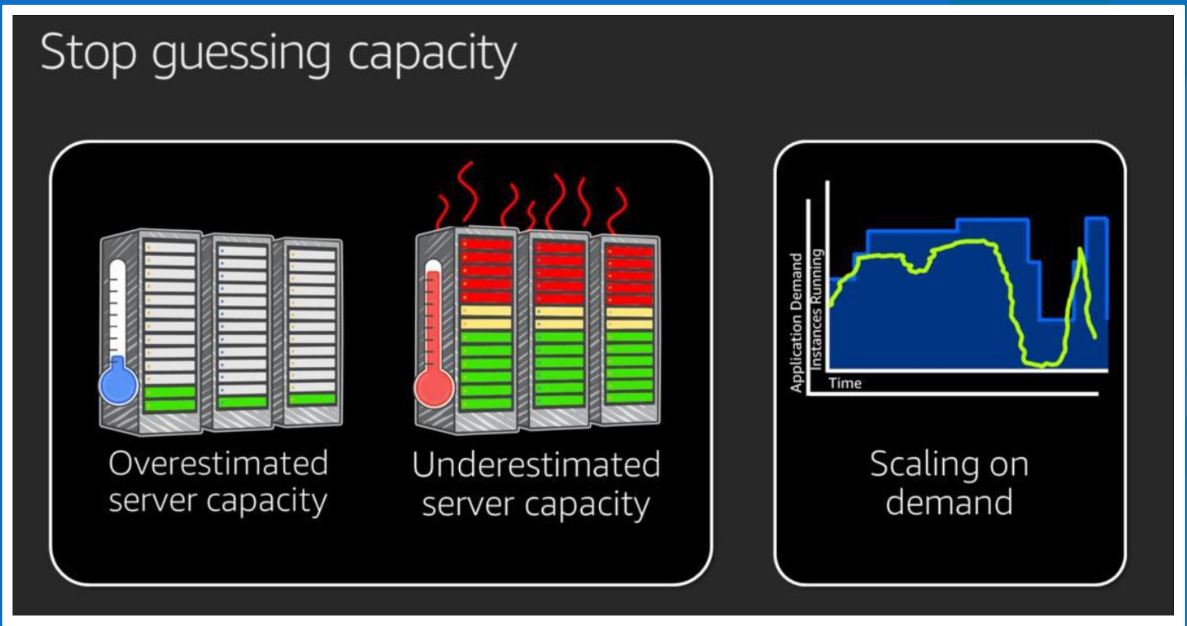
Improved Support

- Easier to support resulting in increased response times; No remote connections
- Data reliability without the maintenance
- Stay current on latest server software
- Stay current on latest virus protections
- Will always have a backup

40

Scalability

41



Stop guessing capacity

Overestimated server capacity

Underestimated server capacity

Scaling on demand

42

Scalability

- Eliminate in-house data servers/centers
  - Higher performance through provisioning resources as needed
  - Unlimited scaling capacity, pay for what you need today with the ability to grow and shrink for maximum capacity scenarios
  - Quit paying for future expenses by over allocating resources not needed today!

43

Reliable Performance

44

Reliable Performance

- Cloud provider monitors sites and overall health
- Speed up processes by staying current on latest technology and not running outdated hardware and software
- No need to worry about disk space; the cloud has massive online storage

For more info/questions, email:

knye@mysoftwaresolutions.com

Housekeeping