The Evolution of Cloud Security

What has changed.

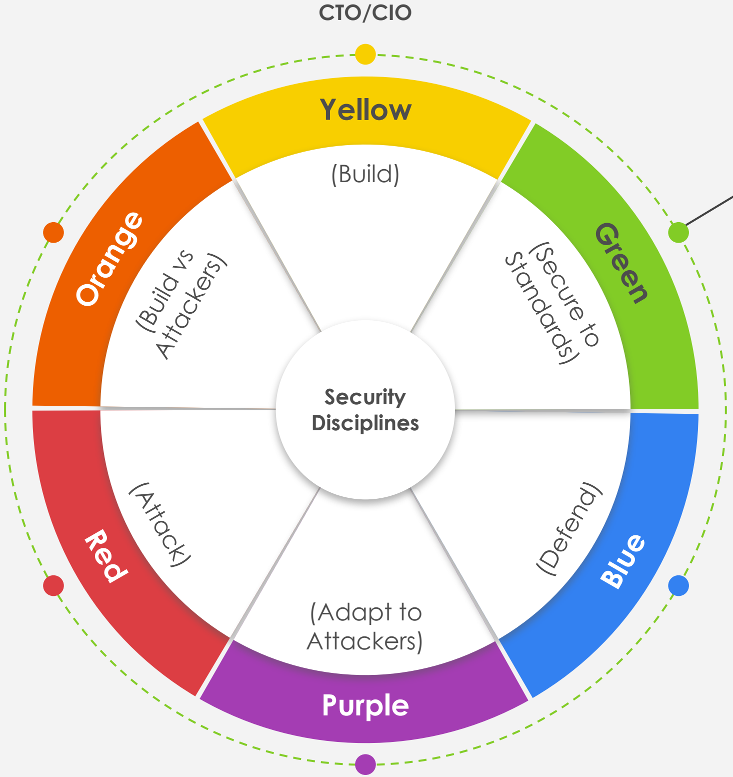
What has not.

Aaron Wilson
Thursday, March 21, 2024
ISACA San Diego

// Hello

- Cofounder @ ScaleSec
- Cloud @ AWS
- SIEM @ ArcSight
- MSSP @ SAIC
- Based in San Diego, CA

// Focus: shipping secure product fast



The InfoSec Color Wheel

Our Green Team Mission:

Address security as efficiently as possible, across as much of the organization as possible.

Current Engagements Snapshot

- Build a global retail payments platform
- Manage cloud incidents
- Provide Tier 1 cloud engineering support
- Launch global secrets management solution
- Build security into cloud infrastructure code
- Take products to federal market: wearable health device, email security platform, cloud call center, bioinformatics automation, software security

Reference: April Wright, Twitter

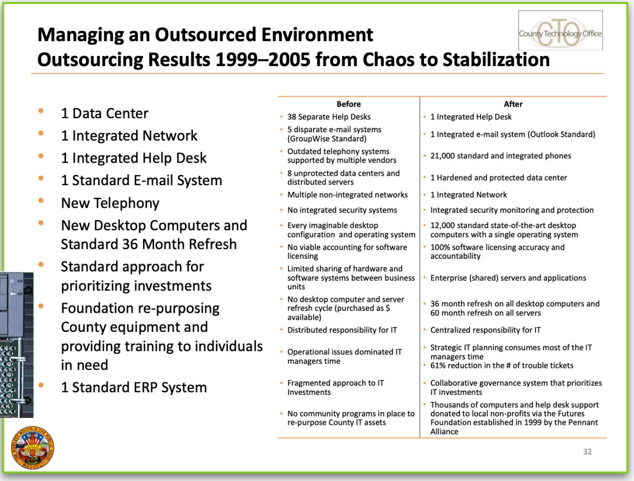
// 2012: I think I know everything.

incident response

threat intelligence

ArcSight

IT outsourcing



CTO County Technology Office

Managing an Outsourced Environment
Outsourcing Results 1999–2005 from Chaos to Stabilization

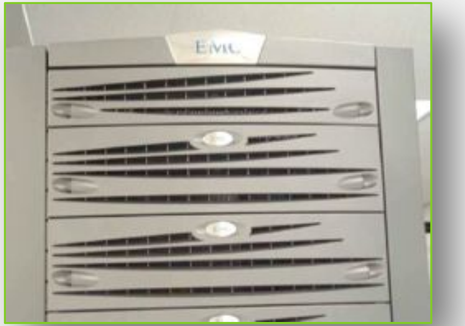
- 1 Data Center
- 1 Integrated Network
- 1 Integrated Help Desk
- 1 Standard E-mail System
- New Telephony
- New Desktop Computers and Standard 36 Month Refresh
- Standard approach for prioritizing investments
- Foundation re-purposing County equipment and providing training to individuals in need
- 1 Standard ERP System

Before	After
38 Separate Help Desks	1 Integrated Help Desk
5 disparate e-mail systems (GroupWise Standard)	1 Integrated e-mail system (Outlook Standard)
Outdated telephony systems supported by multiple vendors	21,000 standard and integrated phones
8 unprotected data centers and distributed servers	1 Hardened and protected data center
Multiple non-integrated networks	1 Integrated Network
No integrated security systems	Integrated security monitoring and protection
Every imaginable desktop configuration and operating system	12,000 standard state-of-the-art desktop computers with a single operating system
No viable accounting for software licensing	100% software licensing accuracy and accountability
Limited sharing of hardware and software systems between business units	Enterprise (shared) servers and applications
No desktop computer and server refresh cycle (purchased as $ available)	36 month refresh on all desktop computers and 60 month refresh on all servers
Distributed responsibility for IT	Centralized responsibility for IT
Operational issues dominated IT managers time	Strategic IT planning consumes most of the IT managers time 61% reduction in the # of trouble tickets
Fragmented approach to IT Investments	Collaborative governance system that prioritizes IT investments
No community programs in place to re-purpose County IT assets	Thousands of computers and help desk support donated to local non-profits via the Futures Foundation established in 1999 by the Pennant Alliance

32

CISCO CERTIFIED CCNA

security engineering

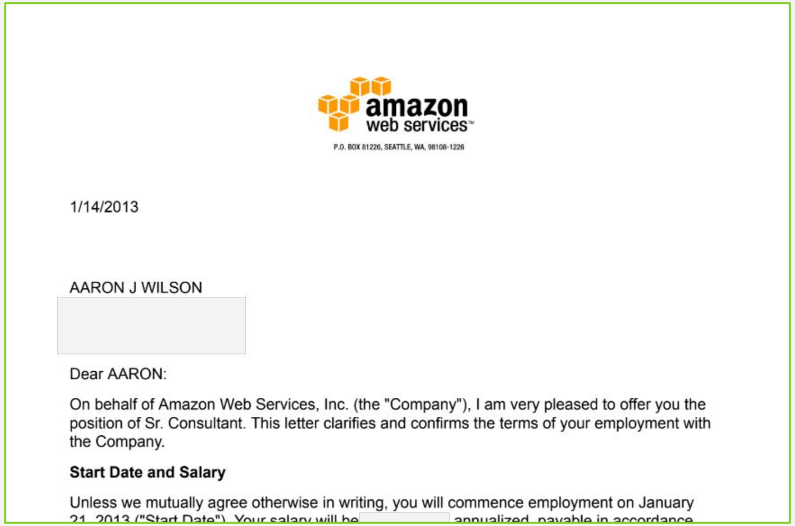


security event correlation & analytics

disaster recovery

ARCHER™

// 2013: I start a new job.



P.O. BOX 81226, SEATTLE, WA, 98108-1226

1/14/2013

AARON J WILSON
[redacted]

Dear AARON:

On behalf of Amazon Web Services, Inc. (the "Company"), I am very pleased to offer you the position of Sr. Consultant. This letter clarifies and confirms the terms of your employment with the Company.

Start Date and Salary

Unless we mutually agree otherwise in writing, you will commence employment on January 21, 2013 ("Start Date"). Your salary will be [redacted] annualized, payable in accordance

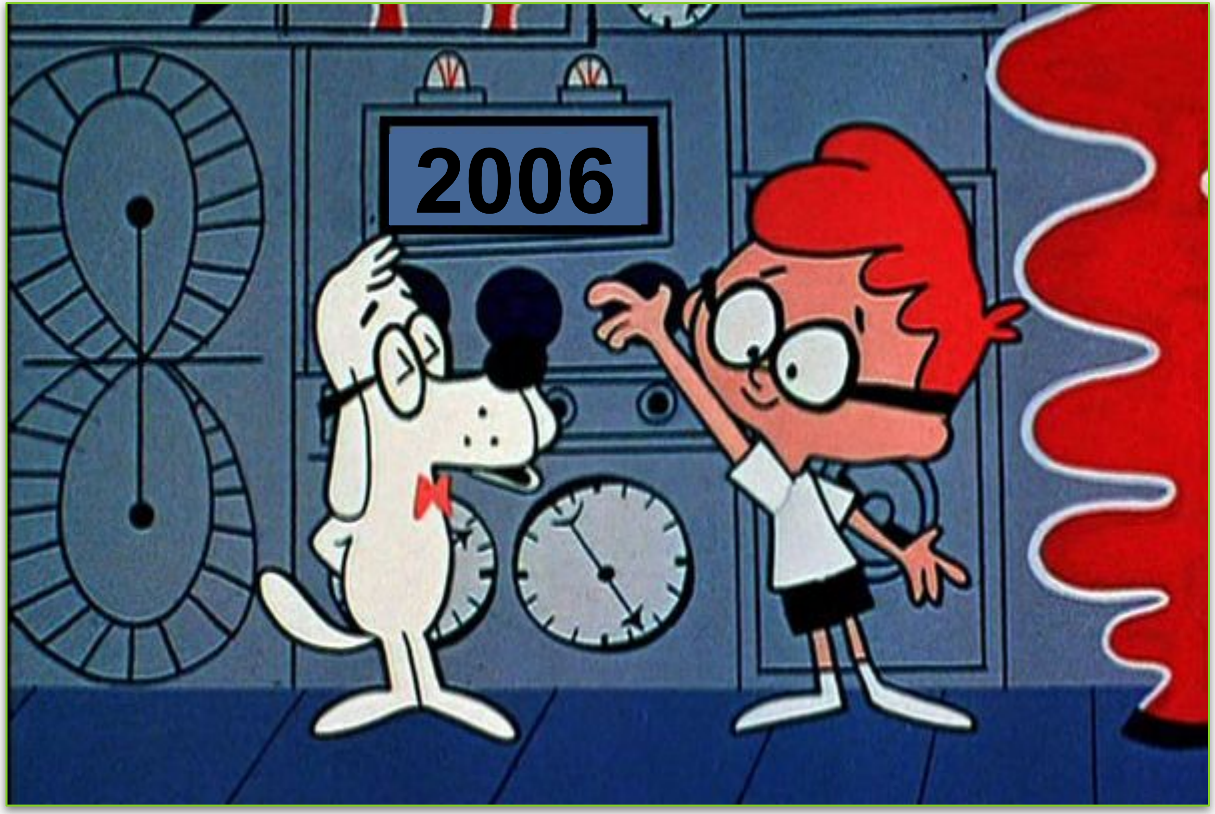
// 2013: I learn I don't know anything.

sea cables

power stations

firmware hacking

substations

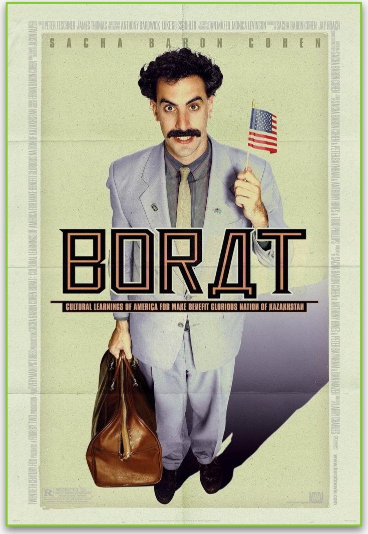

2006

// 2006: AWS Launched

- OK really 2004 if you count preview
- 2005 Mechanical Turk
- July 2006: First infrastructure service GA
- Honorable mention: Alexa Web Information Service (2004-2022)
- 2008 EC2 (conceived in late 2023)

// Also 2006

- Hannah Montana
- Shiloh from Brangelina
- Borat make moviefilm
- Pluto is sad


SACHA BARON COHEN
BORAT
CULTURAL LEARNINGS OF AMERICA FOR MAKE BENEFIT GLORIOUS NATION OF KAZAKHSTAN

ontana

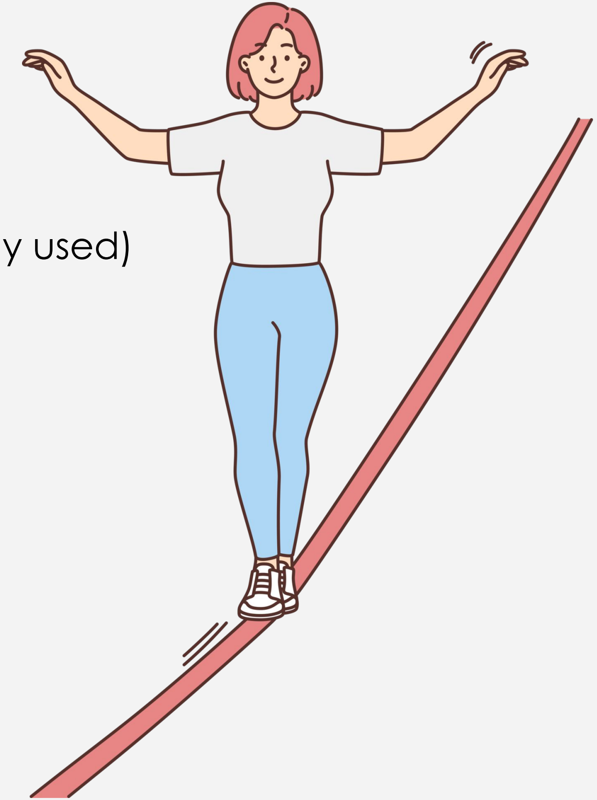
Brangelina

n Brangilina

?

// 2007-2009 Early adopters

- Just a few AWS services available
- Nascent; largely experimental
- EC2 direct on the Internet (VPC GA in 2011)
- No significant security incidents (because it wasn't broadly used)
- Some outages, but services were mostly "beta" then



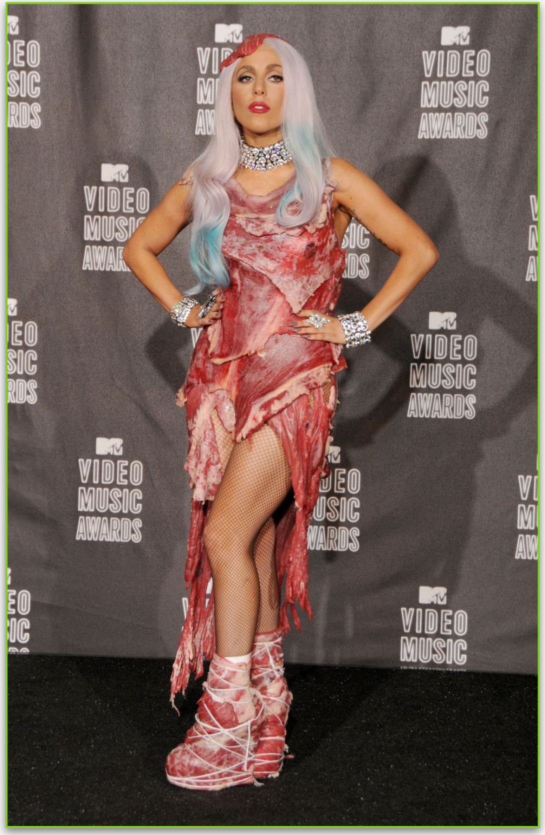
// 2010: Other clouds

Microsoft Azure

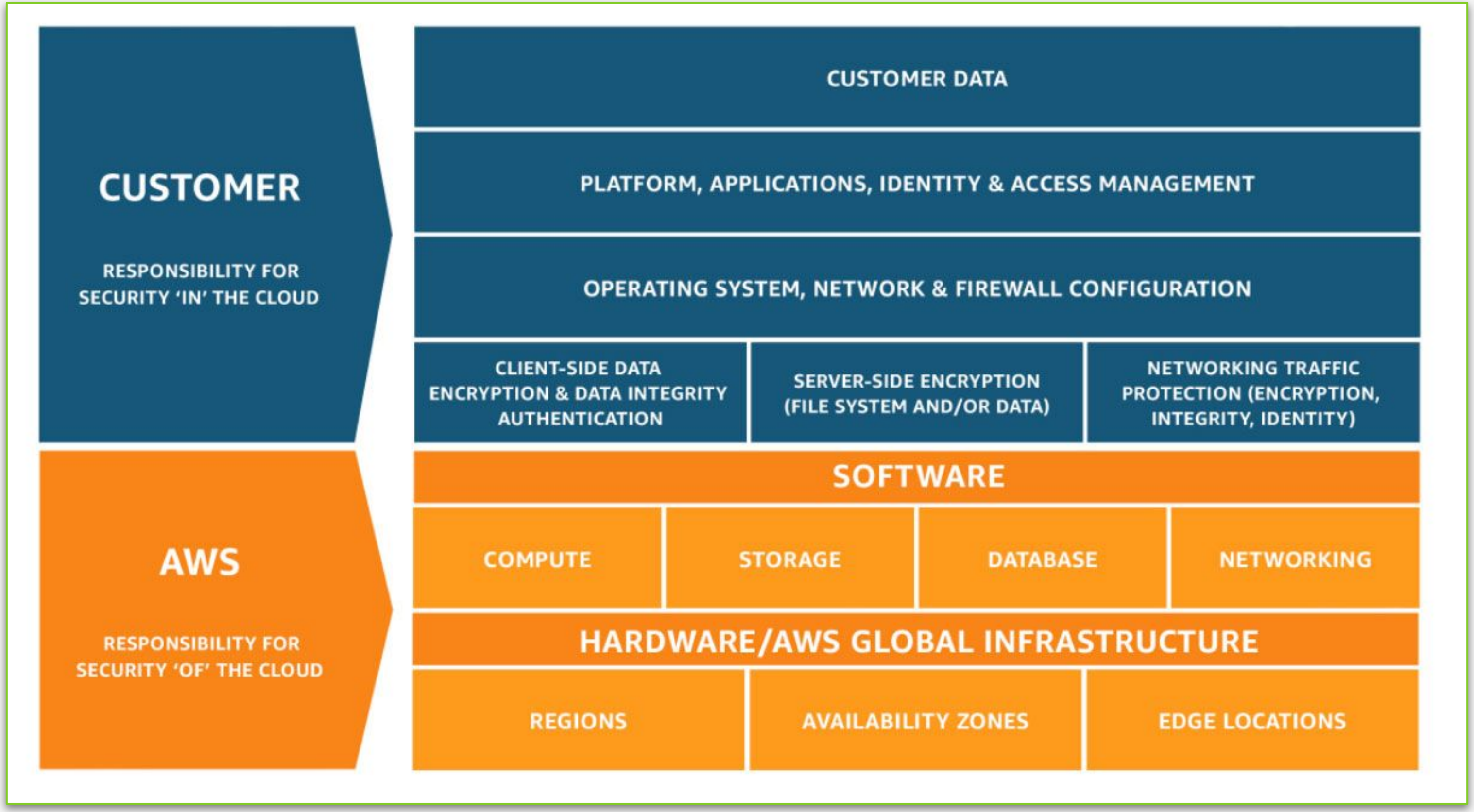
amazon web services

Google Cloud

// Also 2010



// 2012: Shared Responsibility Model



CUSTOMER

RESPONSIBILITY FOR
SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR
SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

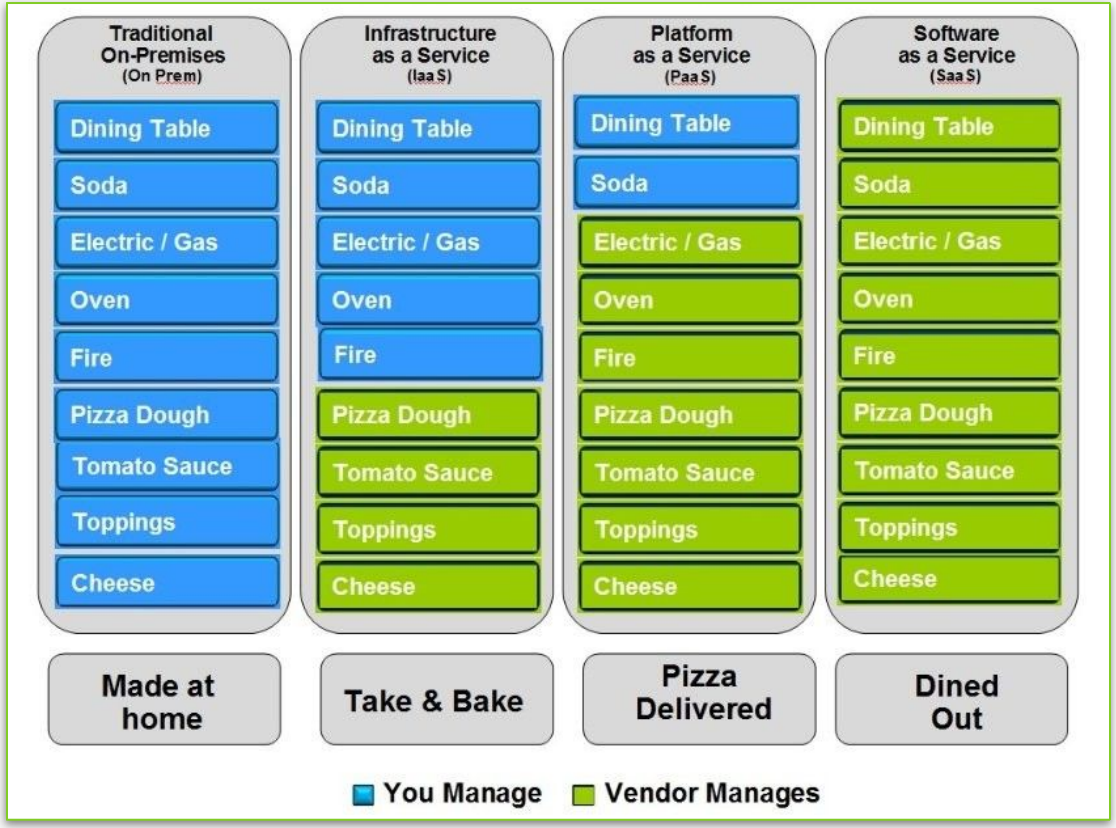
HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

// 2014: Pizza as a Service Model (Albert Barron)



Traditional On-Premises (On Prem)	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
🟦 Dining Table	🟦 Dining Table	🟦 Dining Table	🟩 Dining Table
🟦 Soda	🟦 Soda	🟦 Soda	🟩 Soda
🟦 Electric / Gas	🟦 Electric / Gas	🟩 Electric / Gas	🟩 Electric / Gas
🟦 Oven	🟦 Oven	🟩 Oven	🟩 Oven
🟦 Fire	🟦 Fire	🟩 Fire	🟩 Fire
🟦 Pizza Dough	🟩 Pizza Dough	🟩 Pizza Dough	🟩 Pizza Dough
🟦 Tomato Sauce	🟩 Tomato Sauce	🟩 Tomato Sauce	🟩 Tomato Sauce
🟦 Toppings	🟩 Toppings	🟩 Toppings	🟩 Toppings
🟦 Cheese	🟩 Cheese	🟩 Cheese	🟩 Cheese
Made at home	Take & Bake	Pizza Delivered	Dined Out

🟦 You Manage 🟩 Vendor Manages

// 2013: Travel the world and meet interesting people

"I don't trust the 'cloud'."

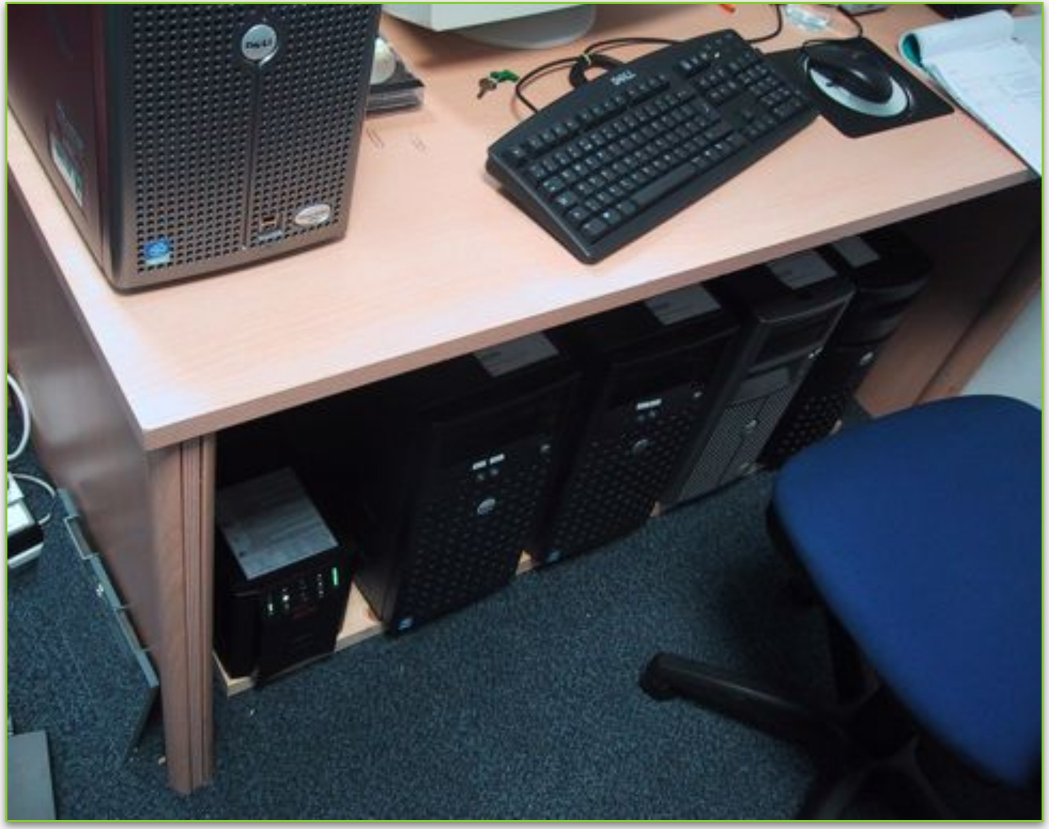
"We were forced to come to this meeting."

"We don't want you here."

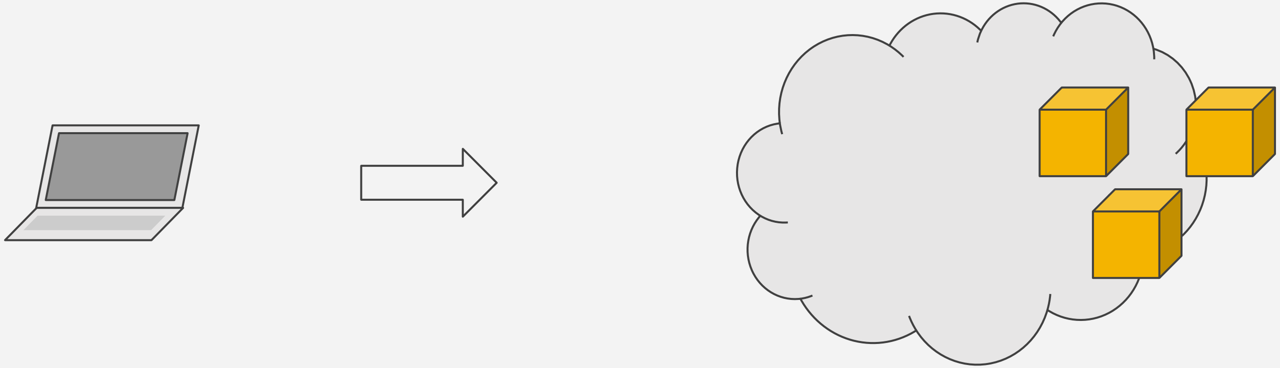
"We don't want cloud."

"Why are people from the bookstore here?"

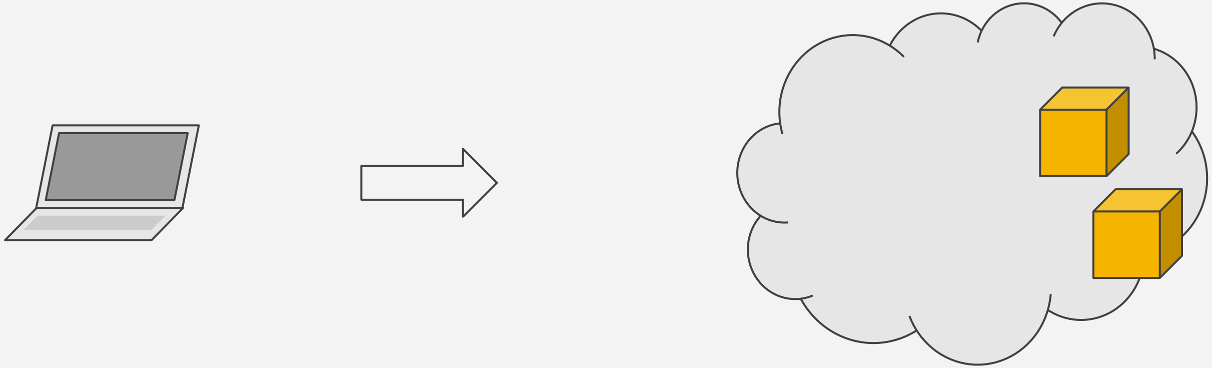
// 2013: "The cloud is not secure"



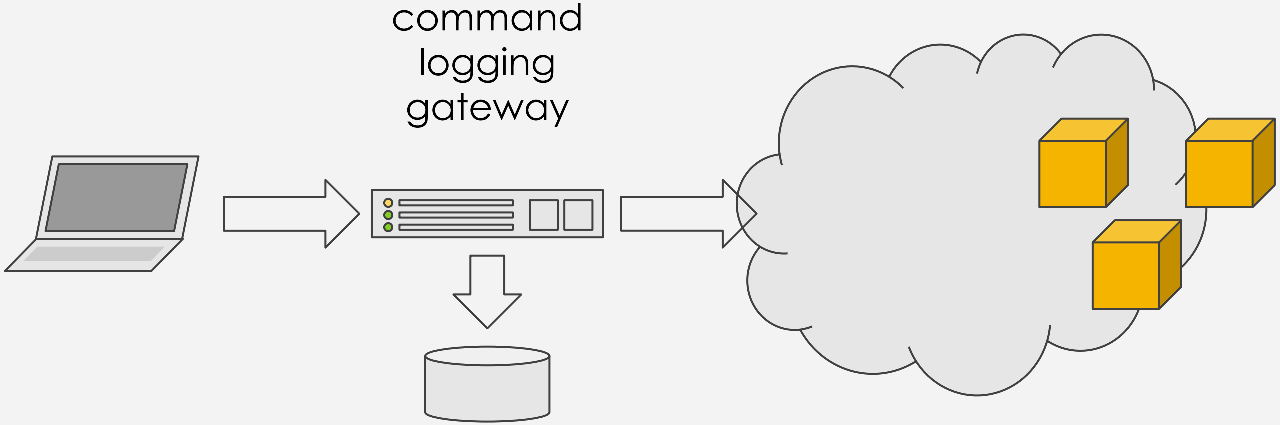
// <2013: Visibility



// <2013: Visibility?

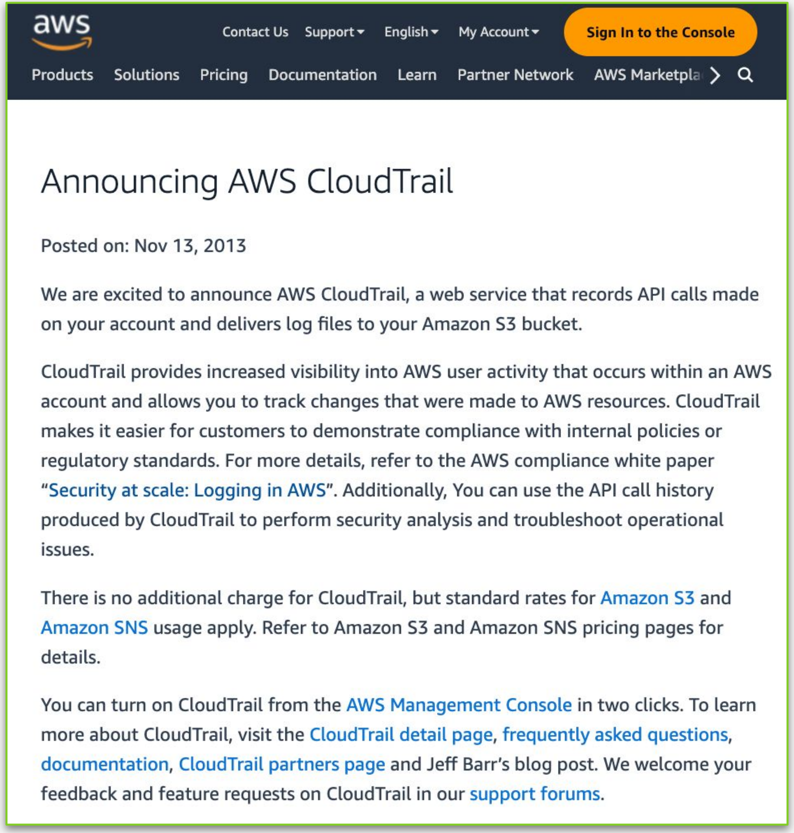


// <2013: Visibility



// 2013+ Visibility

- Records API calls made on an AWS account
  - directly by the user
  - on behalf of the user by an AWS service
- Records logs to your S3 bucket
- AWS CloudFormation, AWS Elastic Beanstalk, AWS OpsWorks, and Auto Scaling, and more



Announcing AWS CloudTrail

Posted on: Nov 13, 2013

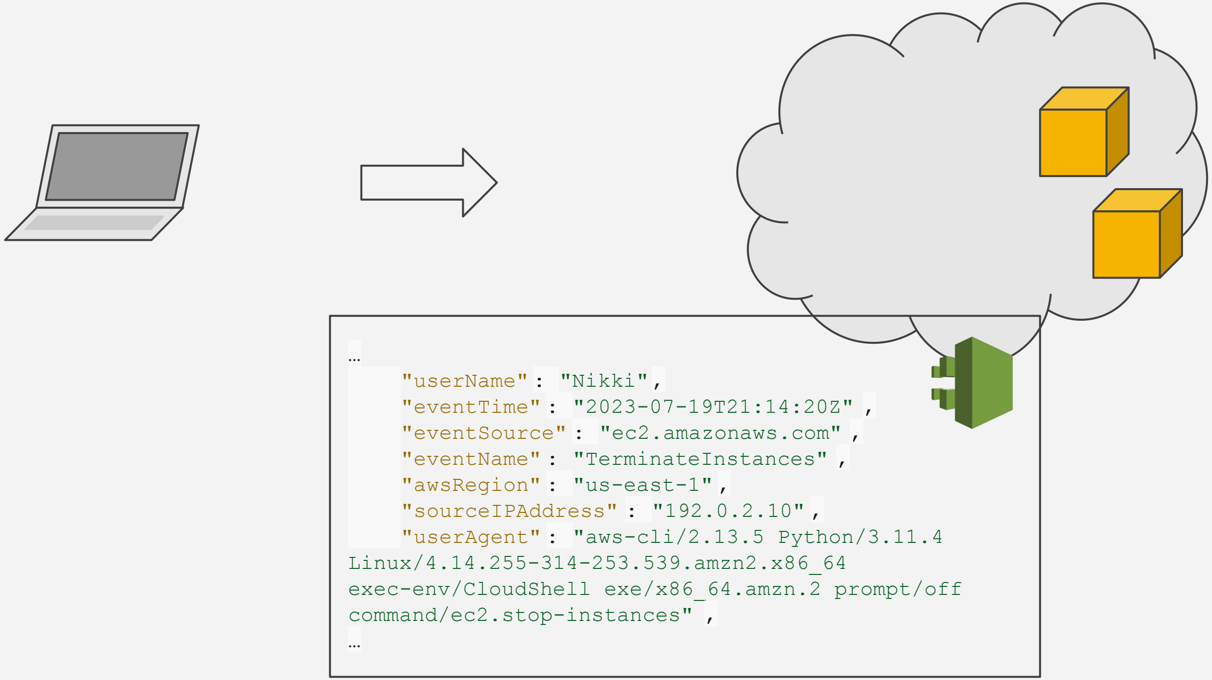
We are excited to announce AWS CloudTrail, a web service that records API calls made on your account and delivers log files to your Amazon S3 bucket.

CloudTrail provides increased visibility into AWS user activity that occurs within an AWS account and allows you to track changes that were made to AWS resources. CloudTrail makes it easier for customers to demonstrate compliance with internal policies or regulatory standards. For more details, refer to the AWS compliance white paper "Security at scale: Logging in AWS". Additionally, You can use the API call history produced by CloudTrail to perform security analysis and troubleshoot operational issues.

There is no additional charge for CloudTrail, but standard rates for Amazon S3 and Amazon SNS usage apply. Refer to Amazon S3 and Amazon SNS pricing pages for details.

You can turn on CloudTrail from the AWS Management Console in two clicks. To learn more about CloudTrail, visit the CloudTrail detail page, frequently asked questions, documentation, CloudTrail partners page and Jeff Barr's blog post. We welcome your feedback and feature requests on CloudTrail in our support forums.

// 2013+ Visibility



```
…
     "userName" : "Nikki",
     "eventTime" : "2023-07-19T21:14:20Z" ,
     "eventSource" : "ec2.amazonaws.com" ,
     "eventName" : "TerminateInstances" ,
     "awsRegion" : "us-east-1",
     "sourceIPAddress" : "192.0.2.10",
     "userAgent" : "aws-cli/2.13.5 Python/3.11.4
Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off
command/ec2.stop-instances" ,
…
```

// 2014: Code Spaces

- Cloud-based code-hosting service
- Attacks
  - Distributed denial of service attack

    And…
  - Destructive attack via AWS console access
- Went out of business in 12 hours
- Partially or completely deleted
  - Virtual machines
  - Data
  - Backups
  - Machine configurations

No MFA?

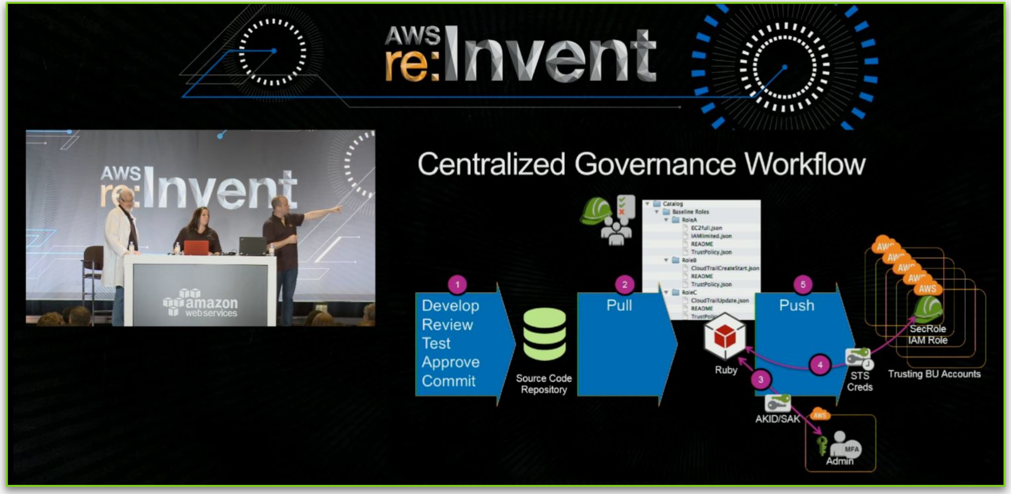
There is no cloud
it’s just someone else's computer

There is no cloud
it’s just someone else’s audit scope

// 2014-2015: Early days of DevSecOps

- Could security solve DevOps challenges?
- Could DevOps solve security challenges?
- Version control
- Automated testing
- Repeatability
- *All the things* as code
    - Security
    - Policy
    - Compliance
    - Change management (ITSM)

AWS & Intuit introducing DevSecOps at re:Invent



DevSecOps powers the Green Team mission!

// Infrastructure trends

virtual machines

2008: Amazon EC2
2012: Azure VMs
2013: GCE

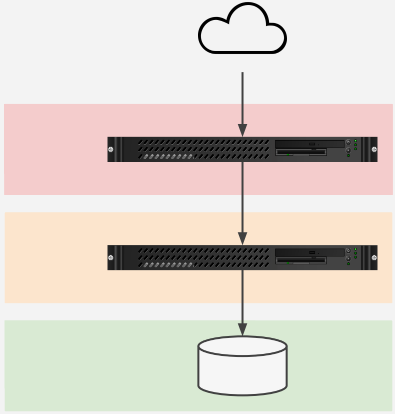
containers

2013: Docker
2014: Kubernetes
2015 Apr: ECS (AWS)
2015 Jul: GKE (GCP)
2017: AKS (Azure)
2017: EKS (AWS)

functions

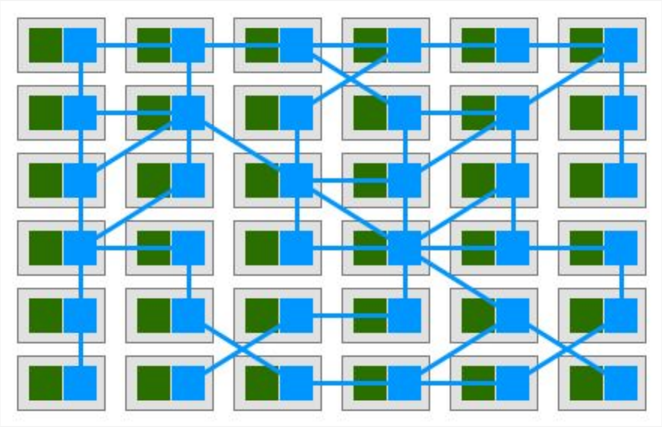
2014: AWS Lambda
2016: Azure Functions
2017: GCP Cloud
Functions

// Workload evolution



3-tier web application

"monolith"



microservices architecture

// 2015-2017: height of data exposure

- US National Geospatial Intelligence Agency - intelligence data, SSH keys, passwords
- CENTCOM / PACOM - 1.8B internet content/histories
- INSCOM - NSA data and DoD battlefield intelligence
- Accenture - internal technical data including VPN keys, dumped hashed passwords
- FedEx - PII for 119k global customers
- Experian - PII and financial data for 123M households
- TigerSwan / Talentpen -defense intelligence, law enforcement info for Vets with clearances
- World Wrestling Entertainment Corp - 3 million emails w/PII
- Chicago Board of Election Commissioners - voter PII, SSNs
- Dow Jones & Wall Street Journal - PII and credit card info for 4M users
- And more…

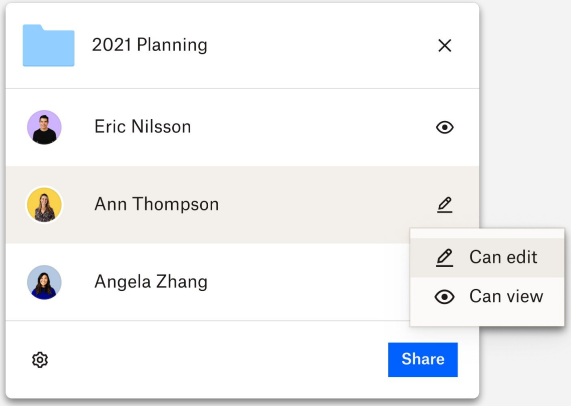
By default, new S3 bucket settings do not allow public access

// Why? Different services for different purposes

Dropbox

!=

amazon S3



storage for humans

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPutObjectS3ServerAccessLogsPolicy",
      "Principal": {
        "Service": "logging.s3.amazonaws.com"
      },
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET-logs/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111111111111"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:s3:::EXAMPLE-SOURCE-BUCKET"
        }
      }
    },
    {
      "Sid": "RestrictToS3ServerAccessLogs",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET-logs/*",
      "Condition": {
        "ForAllValues:StringNotEquals": {
          "aws:PrincipalServiceNamesList": "logging.s3.amazonaws.com"
        }
      }
    }
  ]
}
```

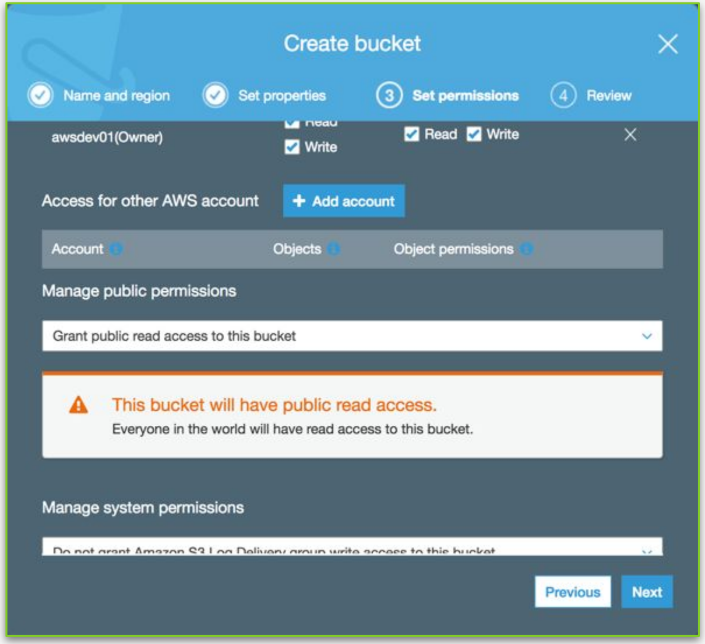
storage for machines

// 2017: S3 security usability enhancement

Nov 6, 2017

The AWS console now highlights all publicly-accessible S3 buckets. Bucket Permissions Check will display the source for the public access (bucket policy, bucket ACLs, or both).

In addition, when you change bucket policy or bucket ACLs, S3 console will analyze them and alert you if those changes will enable public read and write access on the bucket.



awsdev01(Owner) ☑ Read ☑ Write ☑ Read ☑ Write

Access for other AWS account

Account	Objects	Object permissions

Manage public permissions

Grant public read access to this bucket

This bucket will have public read access.
Everyone in the world will have read access to this bucket.

Manage system permissions

Do not grant Amazon S3 Log Delivery group write access to this bucket

// 2017-2019: More S3 security enhancements

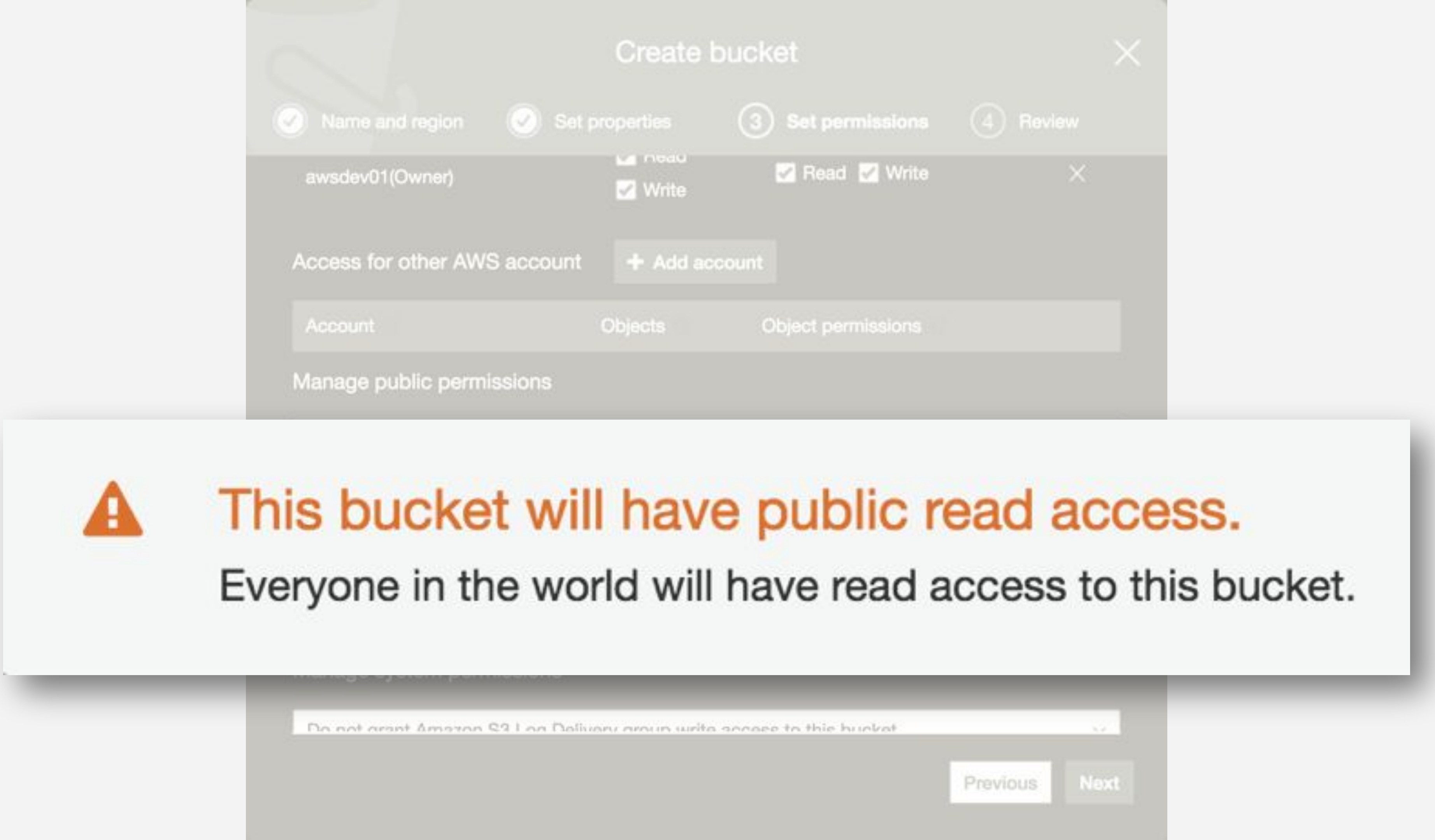
- Aug 14, 2017 AWS Config
  - Check your S3 buckets for unrestricted public access
- Nov 15, 2018: S3 Public Block Access
  - "Centralized control to prevent variation in security configuration"
  - Override S3 permissions that allow public access
  - Every bucket in your account
- Nov 21, 2018: CloudFormation coverage for S3
  - Support for `PublicAccessBlockConfiguration`
- Oct 16, 2019: Amazon GuardDuty
  - Alerts you that S3 block public access was disabled for an S3 bucket

Azure

- Jul 15, 2020: `AllowBlobPublicAccess`

Google

- Dec 15, 2021: `storage.publicAccessPreventio`



awsdev01(Owner) ☑ Read ☑ Write ☑ Read ☑ Write

Access for other AWS account

Account	Objects	Object permissions

Manage public permissions

⚠ This bucket will have public read access.

Everyone in the world will have read access to this bucket.

Manage system permissions

Do not grant Amazon S3 Log Delivery group write access to this bucket

// 2019-2023: EVEN MORE S3 security enhancements

- Access Analyzer for Amazon S3
  - Dec 2, 2019: alerts you when you have a bucket that is configured to allow access to anyone on the internet or that is shared with other AWS accounts
  - Apr 27, 2020: discover S3 buckets that can be accessed publicly or from other accounts or organizations
  - Mar 10, 2021: prevent public and cross-account access before you set permissions
- Amazon Macie (harvest.ai acquired in 2017!)
  - May 13, 2020: 80-90%+ price reduction - inventory buckets and sensitive data
  - May 17, 2021: use criteria to scan existing and future buckets
- AWS Control Tower
  - Apr 8, 2021 - enable the “Block Public Access” setting for all managed buckets

🤯 S3 has new security defaults

  - Announced Dec 13, 2022, activated between Apr 5, 2023 - Apr 28, 2023
  - Block Public Access and disable access control lists (ACLs) for all new S3 buckets

Why did S3 have ACLs in the first place?

2006, 2011

// 2018+: Cryptojacking

- Attacker *finds cloud credentials*
- Launches super powerful VMs
- Installs cryptocurrency mining software
- Starts mining crypto
- Runs up your bill!
  - Less obvious if throttled
  - Maybe on resources/regions you don't use

Tips!

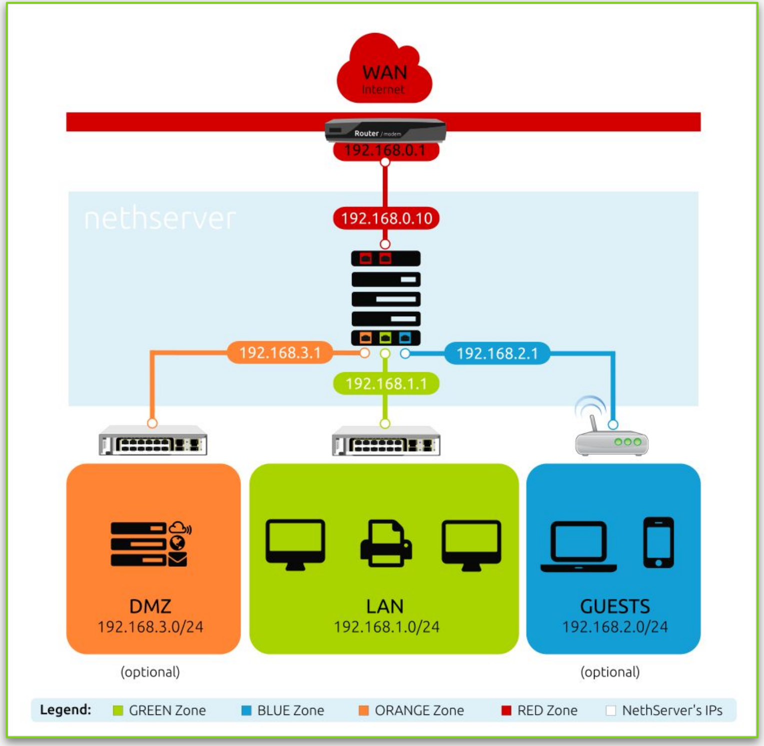
Monitor logs for cloud regions you aren't officially using.

Disable/block cloud services you aren't officially using.

// ~2017-2018: Zero Trust Network Architecture

Authenticate and Control Access
Automate
Protect (Data and Documents)
ZERO TRUST
IDENTITY SERVICE
ENDPOINTS ACCESSING APPS
Stringent Authentication
End to end
ryption
Security
Refinem
Zero Trust Security
veritis
Users
Data
Devices
Zero Trust
Applications
Network Traffic
Components of Zero Trust Framework
Multifactor uthentication 47%
Network analytics 47%
Cloud workload governance 46%
46% Microsegmentation
43% IAM software
40% Least-privilege access
33% Corporate device management
ZERO TRUST
WIFI
CLOUD
ZERO TRUST
ZERO TRUST
SECURITY
WIFI
CLOUD SERVICE
MUTUAL AUTHENTICATION
CHECK
NETWORK
ACCESS

// ~2017-2018: Zero Trust Network Architecture



Traditional high-trust network

NIST SP 800-207

- No implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet)
- No implicit trust or based on asset ownership (enterprise or personally owned)

Key characteristics:

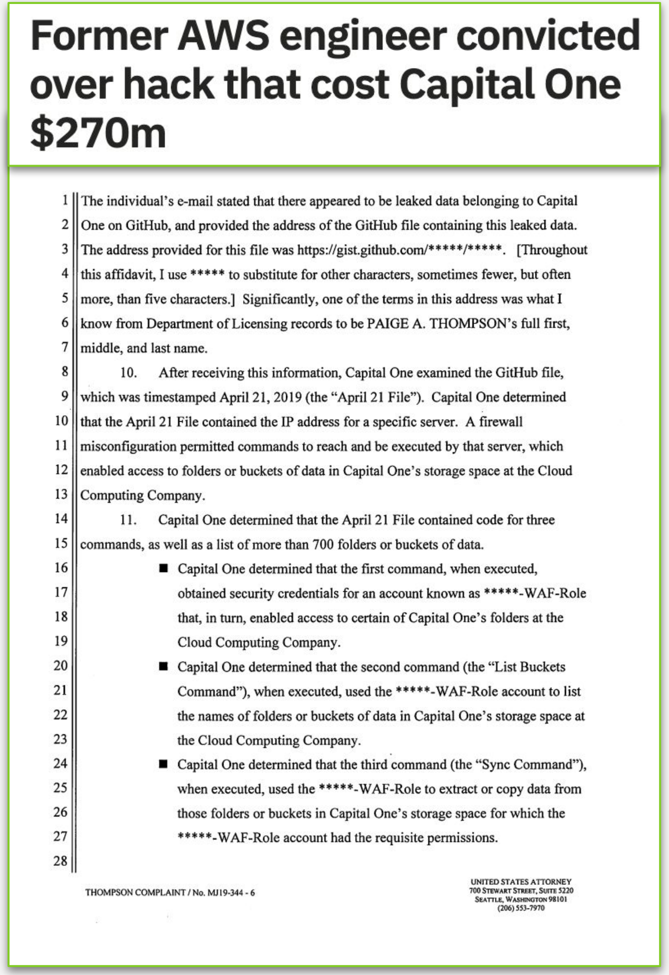
1. Microsegment individual resources
2. Authorize by identity (not IPs)
3. Permit access by least privilege
4. Verify explicitly and continuously
5. Encrypt end-to-end
6. Monitor and automate

Helps address attacks:

- Credential theft
- Phishing attacks
- Lateral movement
- Privilege escalation
- Insider threats
- Data exfiltration

// 2019: Capital One breach

- Capital One breached
- No evidence the data was used for fraud or shared
- 100 million US credit card customers affected
- 1 million Canadian Social Insurance Numbers
- 140,000 Social Security numbers
- 80,000 bank account numbers
- Fined $80M by the Office of the Comptroller of the Currency (OCC)
- Paid $190M for a class action suit
- Years of cleanup



Former AWS engineer convicted over hack that cost Capital One $270m

The individual's e-mail stated that there appeared to be leaked data belonging to Capital One on GitHub, and provided the address of the GitHub file containing this leaked data. The address provided for this file was https://gist.github.com/*****/*****. [Throughout this affidavit, I use ***** to substitute for other characters, sometimes fewer, but often more, than five characters.] Significantly, one of the terms in this address was what I know from Department of Licensing records to be PAIGE A. THOMPSON's full first, middle, and last name.

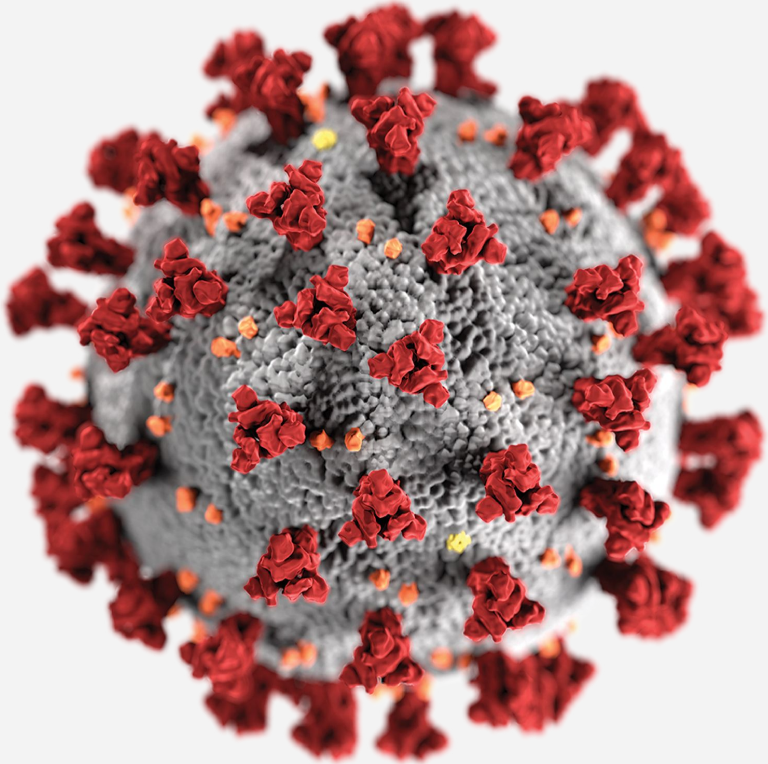
10. After receiving this information, Capital One examined the GitHub file, which was timestamped April 21, 2019 (the "April 21 File"). Capital One determined that the April 21 File contained the IP address for a specific server. A firewall misconfiguration permitted commands to reach and be executed by that server, which enabled access to folders or buckets of data in Capital One's storage space at the Cloud Computing Company.

11. Capital One determined that the April 21 File contained code for three commands, as well as a list of more than 700 folders or buckets of data.

- ■ Capital One determined that the first command, when executed, obtained security credentials for an account known as *****-WAF-Role that, in turn, enabled access to certain of Capital One's folders at the Cloud Computing Company.
- ■ Capital One determined that the second command (the "List Buckets Command"), when executed, used the *****-WAF-Role account to list the names of folders or buckets of data in Capital One's storage space at the Cloud Computing Company.
- ■ Capital One determined that the third command (the "Sync Command"), when executed, used the *****-WAF-Role to extract or copy data from those folders or buckets in Capital One's storage space for which the *****-WAF-Role account had the requisite permissions.

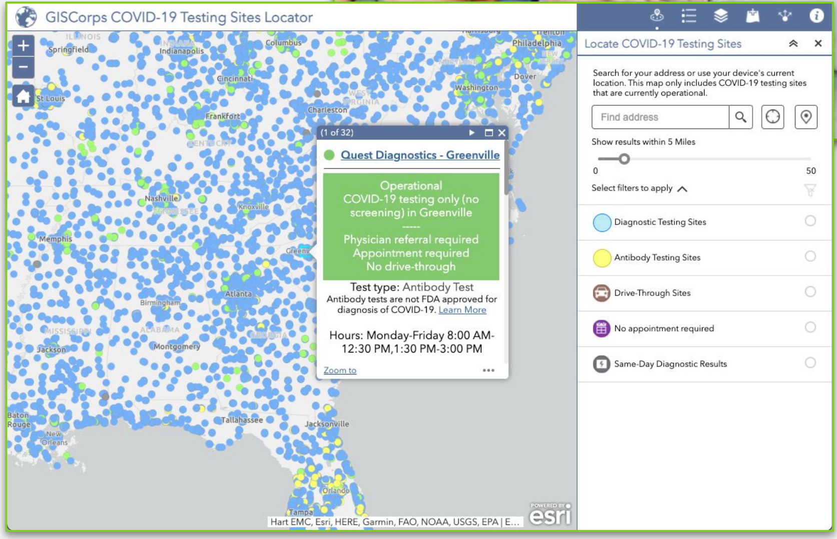
THOMPSON COMPLAINT / No. MJ19-344 - 6

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



// 2020: Working from Home

- Digital entertainment - streaming, games, social
- Remote work & collaboration
- E-Learning
- E-Commerce
- Accelerated cloud adoption & migration
- Remote, distributed operations
- Research collaboration
- Public services



GISCorps COVID-19 Testing Sites Locator

(1 of 32)

Quest Diagnostics - Greenville

Operational
COVID-19 testing only (no screening) in Greenville

Physician referral required
Appointment required
No drive-through

Test type: Antibody Test
Antibody tests are not FDA approved for diagnosis of COVID-19. Learn More

Hours: Monday-Friday 8:00 AM-12:30 PM,1:30 PM-3:00 PM

Zoom to

Locate COVID-19 Testing Sites

Search for your address or use your device's current location. This map only includes COVID-19 testing sites that are currently operational.

Find address

Show results within 5 Miles

0 50

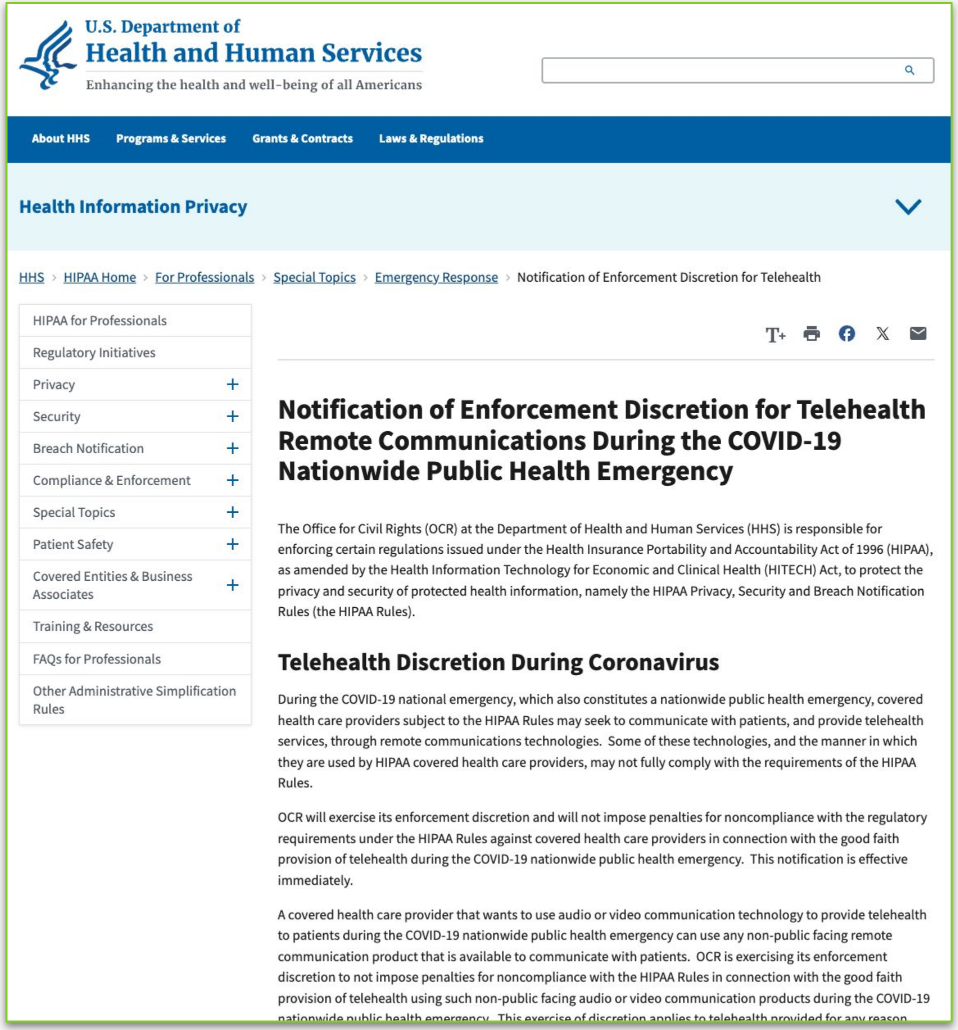
Select filters to apply

- Diagnostic Testing Sites ○
- Antibody Testing Sites ○
- Drive-Through Sites ○
- No appointment required ○
- Same-Day Diagnostic Results ○

Coders Against Covid
findcovidtesting.com

// 2020: Telemedicine

- Office of Civil Rights (OCR) at Health and Human Services (HHS)
- Unprecedented expansion of relaxation of HIPAA enforcement
- HIPAA compliance lifted "in good faith" for apps used for telemedicine like Zoom, Google Meet, FaceTime, Facebook Messenger, Skype, GoToMeeting…
- No telehealth waiver for Facebook Live, Twitch, TikTok, etc.


U.S. Department of
Health and Human Services
Enhancing the health and well-being of all Americans
About HHS
Programs & Services
Grants & Contracts
Laws & Regulations
Health Information Privacy
HHS › HIPAA Home › For Professionals › Special Topics › Emergency Response › Notification of Enforcement Discretion for Telehealth
HIPAA for Professionals
Regulatory Initiatives
Privacy +
Security +
Breach Notification +
Compliance & Enforcement +
Special Topics +
Patient Safety +
Covered Entities & Business Associates +
Training & Resources
FAQs for Professionals
Other Administrative Simplification Rules
T+

Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency

The Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) is responsible for enforcing certain regulations issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, to protect the privacy and security of protected health information, namely the HIPAA Privacy, Security and Breach Notification Rules (the HIPAA Rules).

Telehealth Discretion During Coronavirus

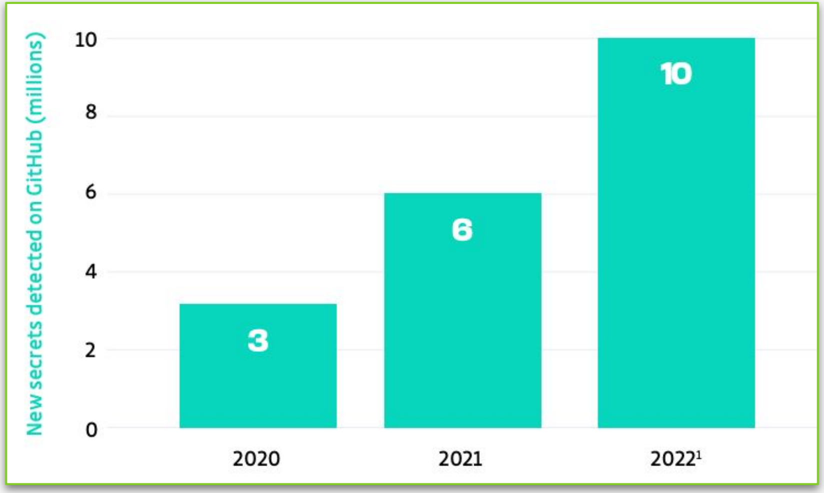
During the COVID-19 national emergency, which also constitutes a nationwide public health emergency, covered health care providers subject to the HIPAA Rules may seek to communicate with patients, and provide telehealth services, through remote communications technologies. Some of these technologies, and the manner in which they are used by HIPAA covered health care providers, may not fully comply with the requirements of the HIPAA Rules.

OCR will exercise its enforcement discretion and will not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules against covered health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency. This notification is effective immediately.

A covered health care provider that wants to use audio or video communication technology to provide telehealth to patients during the COVID-19 nationwide public health emergency can use any non-public facing remote communication product that is available to communicate with patients. OCR is exercising its enforcement discretion to not impose penalties for noncompliance with the HIPAA Rules in connection with the good faith provision of telehealth using such non-public facing audio or video communication products during the COVID-19 nationwide public health emergency. This exercise of discretion applies to telehealth provided for any reason

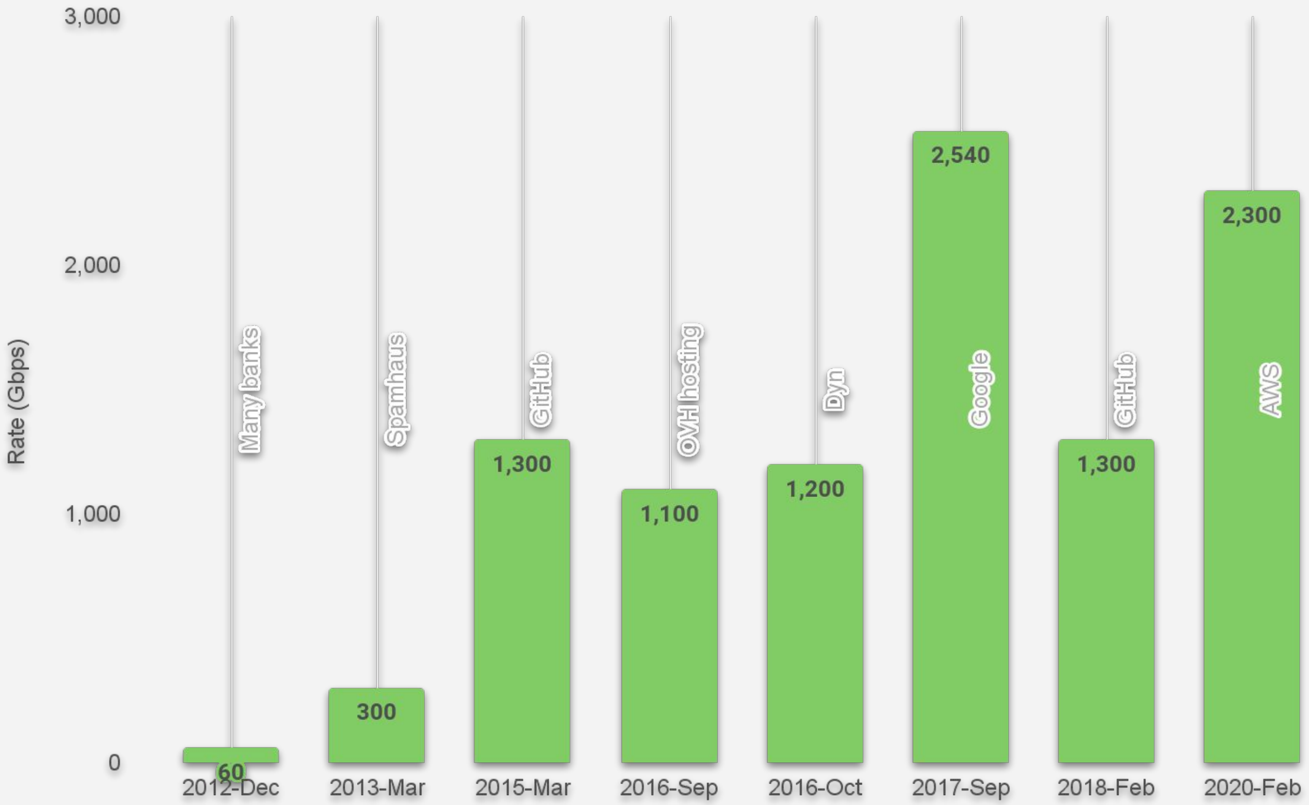
// ~2020-2023 Secrets on GitHub

- Credentials hardcoded into code
  - Generic passwords
  - API keys
  - Access tokens
  - SSH RSA keys
- By design, commit history means removing secrets is non-trivial
- Python, JSON, env, javascript
- Dockerfiles, Kubernetes configs, Terraform, Ansible
- Top offenders are India, China, USA



The State of Secrets Sprawl 2023
GitGuardian

// 2010s-on: DoS (Distributed denial of service) attacks



// Cloud adoption trends

2010-2013	2014-2015	2015-2018	2019-2021	2022-now
Usage: Experimentation and exploration	Building individual business processes, going production	Earnest hybrid and multicloud strategies	Widespread adoption, hybrid and multi-cloud	Optimization and integration, cost management
Security: highly skeptical	Cloud-specific, new enterprise features	More attention to shared responsibility	Measurable, repeatable, code	Predictive, proactive

// Cloud compliance trends: B2B, B2G, regulatory

- 2008: Cloud Security Alliance
- 2010: AICPA SOC 2 (SSAE 16)
- 2011: The NIST Definition of Cloud Computing (SP 800-145)
- 2011: FedRAMP launched by the Office of Management and Budget (OMB)
- 2011: PCI Cloud Computing Guidelines
- 2013: Applying PCI DSS to Cloud Computing Environments
- 2015: ISO 27017 cloud implementation guidance for ISO 27002
- 2016: HHS guidance on HIPAA and cloud computing

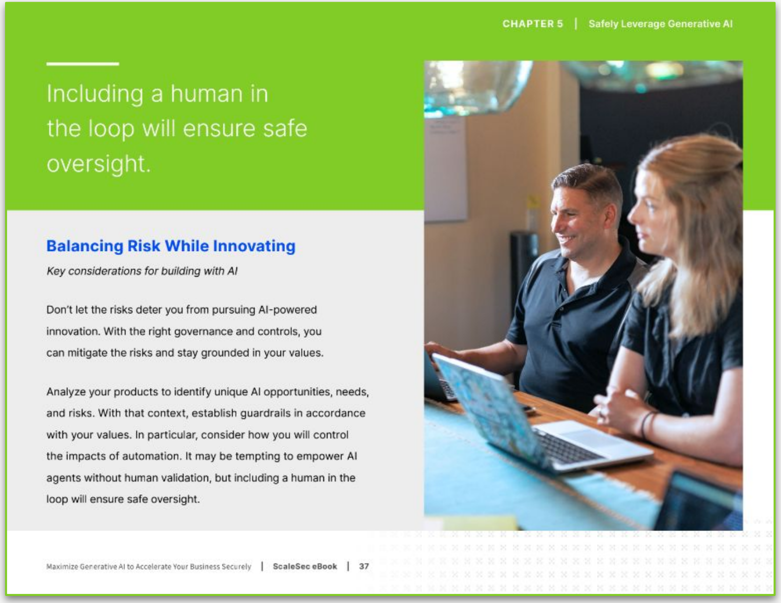
// 2023: AI security

Concerns

- Prompt injection
- Malicious training data
- Hallucinations

Opportunities for cloud security

- Event log analysis
- Anomaly detection
- Policies, reports, documentation
- IR playbooks
- Code analysis and generation
- Forensics analysis



CHAPTER 5 | Safely Leverage Generative AI

Including a human in the loop will ensure safe oversight.

Balancing Risk While Innovating

Key considerations for building with AI

Don't let the risks deter you from pursuing AI-powered innovation. With the right governance and controls, you can mitigate the risks and stay grounded in your values.

Analyze your products to identify unique AI opportunities, needs, and risks. With that context, establish guardrails in accordance with your values. In particular, consider how you will control the impacts of automation. It may be tempting to empower AI agents without human validation, but including a human in the loop will ensure safe oversight.

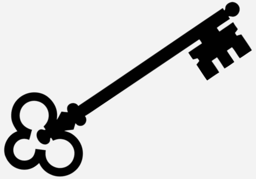
Maximize Generative AI to Accelerate Your Business Securely | ScaleSec eBook | 37

ScaleSec's eBook on using AI securely

// 2023: Microsoft breached by Storm-0558

- China-based actor Storm-0558
- Notified by a customer with Exchange Online anomalies
- Stole Microsoft's consumer certificate authority (CA) signing key
    - Microsoft account (MSA) service
    - MSA powers authentication for all consumer based platforms, like Xbox, outlook.com, etc
    - They aren't sure how
    - Not in a crash dump as previously reported
- Used the key to forge tokens (credentials) for Outlook Web Access and Outlook.com
- Cause: "Developers in the mail system incorrectly assumed libraries performed complete validation and did not add the required issuer/scope validation"
- Microsoft says they took actions to prevent future occurrences, including invalidating the stolen key

> *"...[they accessed] user email from approximately 25 organizations, including government agencies and related consumer accounts in the public cloud."*



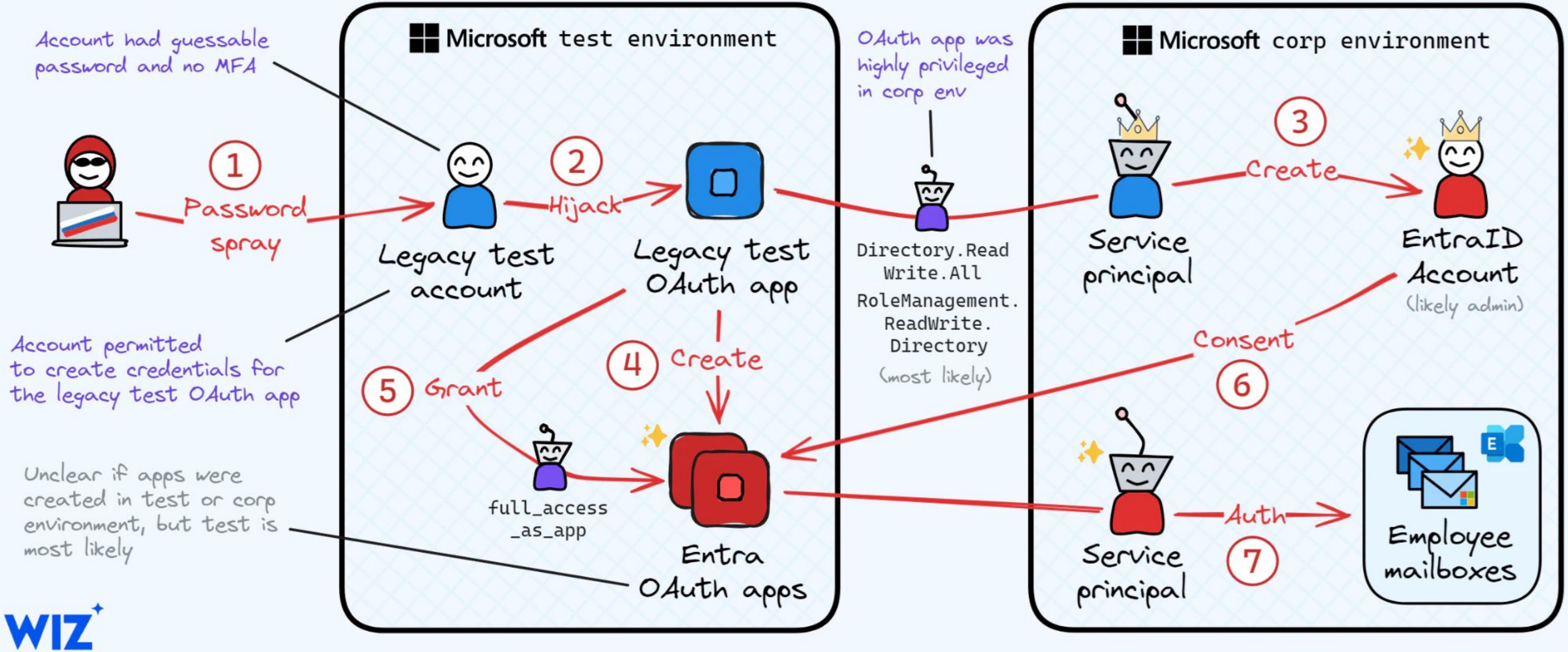
Not in a hardware security module (HSM)?

// 2024: Microsoft breached by SVR

> "...corporate email accounts, including members of our senior leadership team and employees in our cybersecurity, legal, and other functions, and exfiltrated some emails and attached documents…"

- Midnight Blizzard
  - Russia's Foreign Intelligence Service (SVR)
  - Same actors behind 2020 Solar Winds breach
- Jan: broke into corporate email and obtained passwords that Microsoft had emailed to customers
- Breached Microsoft's test environment, then gained access to Microsoft's Corporate environment
- Mar: Now using those passwords to attempt logins (spraying)

Midnight Blizzard Exchange Online Exfiltration Campaign (estimated attack flow)


Account had guessable password and no MFA
1
Password spray
Microsoft test environment
Legacy test account
2
Hijack
Legacy test OAuth app
Account permitted to create credentials for the legacy test OAuth app
5
Grant
4
Create
full_access_as_app
Entra OAuth apps
Unclear if apps were created in test or corp environment, but test is most likely
OAuth app was highly privileged in corp env
Directory.Read Write.All
RoleManagement. ReadWrite. Directory
(most likely)
Microsoft corp environment
Service principal
3
Create
EntraID Account
(likely admin)
Consent
6
Service principal
Auth
7
Employee mailboxes
E

WIZ

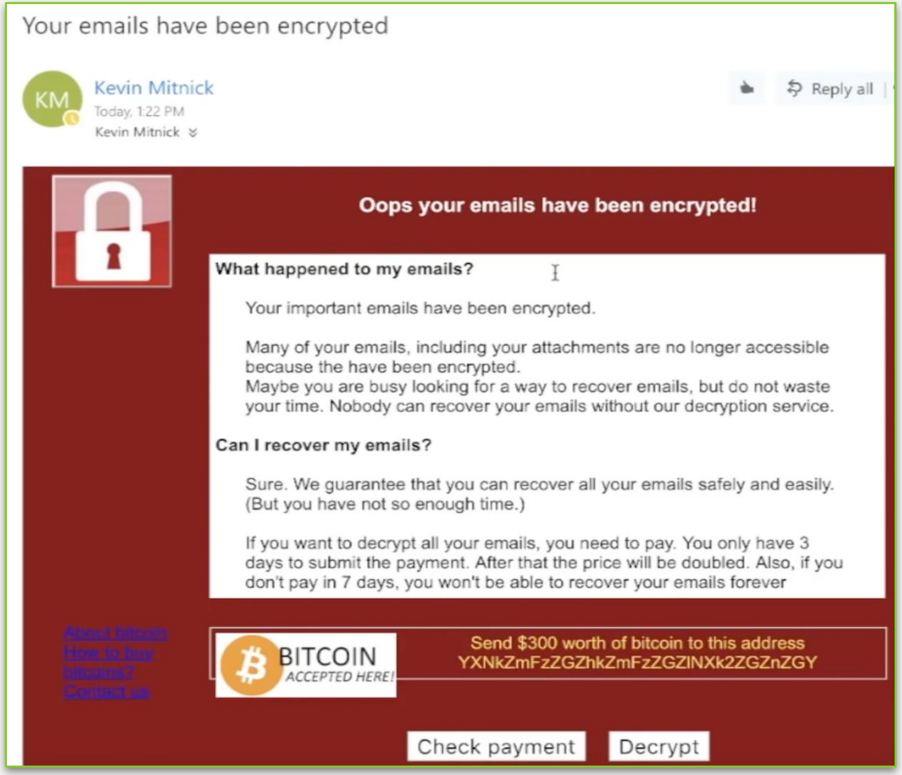
// The future…

Expect little change for:

- Misconfigurations by cloud customers
- Confusion about the shared responsibility model
- Supply chain attacks
- Breaches of privileged tools
    - E.g. Solar Winds
- Unintentional data/secrets exposure

Emerging

- AI-powered attacks
- "Ransomcloud" coming soon…



Your emails have been encrypted

Kevin Mitnick
Today, 1:22 PM
Kevin Mitnick

Oops your emails have been encrypted!

What happened to my emails?

Your important emails have been encrypted.

Many of your emails, including your attachments are no longer accessible because the have been encrypted.
Maybe you are busy looking for a way to recover emails, but do not waste your time. Nobody can recover your emails without our decryption service.

Can I recover my emails?

Sure. We guarantee that you can recover all your emails safely and easily. (But you have not so enough time.)

If you want to decrypt all your emails, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your emails forever

About bitcoin
How to buy bitcoins?
Contact us

Send $300 worth of bitcoin to this address
YXNkZmFzZGZhkZmFzZGZINXk2ZGZnZGY

// Closing thoughts

Advice

- Buy more than you build
- Get a hardware key MFA
- Use a password manager for humans and use a secrets manager for apps
- Inventory and inspect public code repositories
- Harden cloud tenants and turn on security services
- Prevent misconfigurations and secrets leaks

Blog: Harden cloud services

(March 2022 White House statement)

// Thanks!

Aaron Wilson

Cloud Security Leader