The Shift to Cloud Computing - Implications for Enterprises and Threat Detection with AWS

Maia Frazier

University of Arizona

[redacted]

Abstract

An enterprise transitioning on-premise resources to the cloud presents advantages such as scalability, savings on initial hardware investments, and having a wide variety of cloud services and providers to choose from. However, the transition from on-premise to the cloud presents additional complexities for cost, compliance, and especially security configurations. With adapting to a new cloud platform, enterprises may encounter difficulty understanding cloud platform-specific controls for security, or familiarity with additional cloud tools for logging and threat detection. This paper will address the gap in cloud computing threat detection research through the exploration of services in AWS. This exploration will leverage logging, a custom Windows PowerShell script, built-in tools for logging and threat hunting such as CloudWatch and GuardDuty, and the provisioning of a vulnerable virtual machine to analyze and visualize security event logs.

Table of Contents

Table of Figures

The Global Shift Towards Cloud Computing

The global shift towards cloud computing is projected to rapidly expand in the upcoming years. According to the International Data Corporation's Worldwide Software and Public Cloud Services Spending Guide, worldwide spending on public cloud services alone is expected to double from an estimated 805 billion in 2024, to 1.61 trillion by 2028 (Shirer, 2024). The cloud industry has expansive options, with private, public, and hybrid models providing varying levels of cloud involvement. Additionally, there are many cloud service options to choose from, such as Software, Infrastructure, Platform, Security, and various other XaaS offerings, by a large selection of Cloud Service Providers (CSPs). While the continued success of the cloud industry presents growth opportunities for enterprises, there is additional complexity associated with migrating resources into the cloud. Cloud computing services, such as Amazon Web Services, offer platforms for extensive monitoring and logging of virtual resources, enabling enhanced threat detection and analysis of attack strategies by malicious actors. However, the transition from an on-premises infrastructure to a cloud solution must be carefully considered by an enterprise in regards to compliance, cost, and security concerns to guarantee successful deployment.

An Introduction to Cloud Computing

A cloud computing model offloads the requirement of having certain resources on premises, such as storage, servers, or other network resources, and uses those of a Cloud Service Provider. There are several essential characteristics of what a cloud service must contain. As defined by the National Institute of Standards and Technology (NIST), these are on demand self-service, broad network access, resource pooling, rapid elasticity, and measured service (Mell &

Grance, 2011). A Cloud Service Provider (CSP) is an entity that owns large data centers that allow customers to have access to virtualized resources, rather than needing to own the physical hardware. For example, an enterprise may need to launch a new web application, without purchasing an additional server. The enterprise can deploy an Amazon Elastic Compute Cloud (EC2) instance, to deploy a new web application in the cloud. With the advantage of a reduced upfront investment in hardware, cloud computing becomes an appealing option for being able to accomplish infrastructural needs, without the purchase of additional hardware.

Cloud Computing Deployment Models

Cloud computing services can be based on a few different deployment models: public, private, community, and hybrid. A public cloud model exists on the premises of the CSP, and can be used by the general public, with Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Computing (GCP) being well known examples of CSPs providing public cloud models (Mell & Grance, 2011). A private cloud model is deployed for use by a single organization only, can be managed and owned by either the organization, a third party, or both, and can be held on or off premise (Mell & Grance, 2011). A private cloud may be necessary if an organization has sensitive patient data to protect, for example, a hospital needing to remain HIPAA compliant (IBM, 2024). A community cloud model is deployed for the use of a specific group of consumers who hold something in common, for example, their mission, or their compliance requirements. It can be owned or managed by any of the organizations in the shared community, a third party, or a combination of the two, and can be held on or off premise (Mell & Grance, 2011). The previous example of a private cloud service being deployed for protecting patient data can be extended in community clouds, with a group of hospitals sharing the

resources of a community cloud to store patient data securely and remain HIPAA compliant. The final cloud deployment model is the hybrid model, which is a combination of two or more private, public, or community clouds (Mell & Grance, 2011). An example of a hybrid cloud model can be seen in Disaster Recovery approaches, when an enterprise hosts their systems and data in a private cloud, and backs up their infrastructure on a public cloud. If there is a disaster, the enterprise can migrate their operations to the public cloud to continue running with minimal disruption (IBM, 2023). The deployment model selected by an enterprise will influence how it is integrated into their infrastructure, since they have differing levels of on-premise involvement.

Cloud Computing Service Models

There are three primary service models in cloud computing: Software as a Service, Infrastructure as a Service, and Platform as a Service. Software as a Service provides a consumer with the ability to use the CSP's applications on the cloud infrastructure. These applications may be accessed through interfaces such as a web browser or a program (Mell & Grance, 2011). Examples of Software as a Service include applications such as Zoom, Slack, and DropBox. Infrastructure as a Service provides consumers with the ability to provision computing resources for things such as servers, networking, or storage (Mell & Grance, 2011). The three major cloud platforms, AWS, Azure, and Google Cloud Platform all provide Infrastructure as a Service. With the Platform as a Service model, consumers can deploy their own applications onto the cloud (Mell & Grance, 2011). An example of PaaS is AWS Lambda, a service that allows for running code without the need of provisioning servers (SpiceWorks, 2025). In addition to the three main service models, there is the concept of "anything" as a service, or XaaS. This term can be applied to any kind of service model that is not considered SaaS, PaaS, or IaaS. For example, Databases

as a Service (DBaaS), Containers as a Service (CaaS), or Storage as a Service (STaaS) are all types of additional service models that can be provided by a CSP (Flinders & Smalley, 2024).

Literature Review

Cloud Security Alliance - Top Threats to Cloud Computing 2024 Report

The Cloud Security Alliance is a leading organization in research and publications related to cloud security. Each year, it publishes a report for the most common security threats found throughout the year across hundreds of vendors. Their 2024 report covers the top 11 security threats, surveying 500 industry experts (CSA, 2024). This yearly report is a useful resource for examining the evolution of the top cloud vulnerabilities, as the ranking of them typically changes from year to year. Enterprises utilizing cloud resources can benefit from being up to date with this report, as they can remain knowledgeable about the top cloud security threats and their respective mitigations as they evolve.

There are 11 threats mentioned in total, with the top three being Misconfiguration and Inadequate Change Control, Identity and Access Management, and Insecure User Interfaces (CSA, 2024). For each of these, the business impacts, key takeaways, and anecdotes/examples are provided. Misconfiguration and Inadequate Change Control being the top concern highlights the need for enterprises to implement stronger, uniquely tailored configurations in their cloud environments, and to be fluent in what dynamic cloud computing configurations require. Identity and Access Management contains components like single sign on, multi factor authentication, authentication, and authorization, increasing the granular complexity of an enterprise's infrastructure. To mitigate this security risk, the CSA recommends unifying IAM solutions, implementing least privilege, automating the provisioning and deprovisioning of accounts and permissions, and implementing automated tools to monitor account lifecycles (CSA, 2024). An

area of improvement for the CSA report could be more transparency into who exactly the 500 industry experts are, and potentially surveying more than 500 to further validate their surveys.

NSA - Manage Logs for Effective Threat Hunting

This document from the NSA emphasizes the importance of log management for securing cloud infrastructures. It cites MITRE's D3FEND and ATT&CK Matrixes when providing explanations for how proper log management can be applied in detecting certain threat tactics, and it provides their countermeasures. It highlights the benefits of maintaining proper logging, such as investigating security incidents, and meeting compliance and audit requirements. The document also details the balance between understanding what kinds of logs need to be enabled, as enabling many kinds of logging can be resource intensive. The NSA asserts that logging should be enabled for critical applications, hosts, networks, and cloud API calls. It also emphasizes the need for logging based on event type, and descriptions of several of these event types, including user and resource actions, security, error, performance, compliance, and billing events (NSA, 2024). The NSA recommends the use of SIEM, a Security Information and Event Management system, and a SOAR, a Security Orchestration Automation and Response tool for processing logs and configuring alerting. It provides a nine-step guide in log collection and analysis: identify sources for security events, enable, review, and adjust logging settings, collect and store logs from selected sources, normalize and enrich logs, analyze logs with a designated tool, correlate logs, perform active threat hunting, support vulnerability assessment and penetration testing, and create queries and alerts. This guide can be a useful resource for enterprises looking to improve their methods for log collection and analysis. The threat of log removal from adversaries is used to demonstrate the relevance of proper log management. An

area of improvement for the NSA document could be providing specific examples of typical SIEM or SOAR applications, beyond introducing them as a concept.

CrowdStrike - 2025 Global Threat Report

CrowdStrike's 2025 threat hunting report includes a section dedicated to examining how threat actors have continued to increase the sophistication of their cloud targeted attacks. CrowdStrike asserts that the volume of observed cloud-focused attacks has increased, as more enterprises shift to the cloud. A few of the trends CrowdStrike notes from 2024 include gaining access from valid accounts, utilizing cloud management tools to gain lateral movement, and abuse of CSP command line tools (CrowdStrike, 2025). This reporting on the state of cloud security focuses more on the actions of specific Active Persistent Threat (APT) groups, their tactics, and if there has been either an increase or decrease in observance of their activity. Some of the groups mentioned include SCATTERED SPIDER, China-nexus, and LABYRINTH CHOLLIMA. It continues to highlight differences in the tactics used across these groups, emphasizing that strategies for exploiting cloud environments are based on a specific APT.

The top technique observed for this year's report was abusing valid accounts, which occurred in 35% of cloud incidents for the first six months of 2024. To gain the credentials for these accounts, threat groups were observed exploiting unsecured cloud resources, such as the cloud VM Instance Metadata Service, IT Development Services, and password managers. Connections between business partners and cloud tenants were also a source for gaining access credentials (CrowdStrike 2025). An area of improvement for the CrowdStrike report is further explanation of technical terminology. For example, when the authors reference the malware Stealc, it is only mentioned by its name with no further context that it is malware. In general, this

report is written for an audience with a technical background, and the style of writing reflects that.

Comparison of Resources

The document from the NSA is a guide for organizations to understand where logging should be enabled in their cloud services, contrasting the report by the CSA for understanding the overall threat landscape of cloud computing. Both resources from the NSA and CSA cover how to use logging for monitoring cloud resources, supporting that the lack of proper logging and log management is a prevalent issue across cloud computing, and should be addressed by any enterprise looking to integrate cloud services into their infrastructure. These three publications all focus on different aspects of the current state of cloud security, but all support the claim that threat actors commonly take advantage of misconfigured cloud environments, third party services, and a lack of understanding of these environments from the enterprises that deploy them. An organization must remain vigilant and work to deepen their understanding of hardening their cloud resources to ensure that they do not become vulnerable to cloud specific attacks. By staying up to date with the actions of recent APTs, the top security vulnerabilities in cloud environments, and techniques to proactively threat hunt, enterprises are putting themself at an advantage when securing their resources in the cloud.

Cloud Complexity

Migrations to the cloud provide enterprises the benefit of flexibility, scalability, and on-demand access to cloud services. However, migrations bring additional complexity to an enterprise's existing on-premise infrastructure. This is especially true for hybrid cloud environments, which have grown in use by enterprises, due to its combining of both public and

private cloud infrastructures (CSA, 2025). Difficulty encountered by enterprises migrating and maintaining their resources in the cloud has brought about the term “cloud repatriation”, which is observed when companies migrate away from the cloud and back to an on-premise infrastructure. Causes of cloud repatriation include unexpected costs, difficulty complying with internal regulations, storage costs, and a weaker sense of control over enterprise resources in the cloud (Zgola, 2023). Cloud complexity can be best managed by a carefully planned transition into the cloud, and continuous monitoring of the performance of an infrastructure after the transition.

Cloud Governance

The complexity of the cloud has created the need for Cloud Governance. Cloud Governance refers to a framework designed to guide enterprises in their cloud migrations, which has six principles: financial management, cost optimization, operational governance, performance management, asset and configuration management, and security and incident management (Alvarenga, 2023). It is an ongoing process, as integrations into the cloud should be continuously monitored even after deployment. Examples of cloud governance frameworks include COBIT5 for IT governance, and COSO for internal controls (Alvarenga, 2023). In large enterprises, a dedicated team of employees is typically required to carry out cloud governance. However, for smaller to medium sized businesses, cloud governance may become a responsibility shared amongst multiple employees with relevant skills and knowledge, without a designated team. If needed, an enterprise may also consult third party firms for establishing an appropriate cloud governance framework to follow. Implementing a governance framework can help to create a stronger sense of confidence in migrating resources to the cloud, as there are substantial plans in place for the six principles of cloud governance.

Shared Responsibility Model

It is common for CSPs to implement a "shared responsibility model" for responsibilities such as security, or compliance and regulations. AWS's statement on this model is as follows: "AWS is responsible for securing the underlying infrastructure that supports the cloud and the services provided; while customers and APN partners, acting either as data controllers or data processors, are responsible for any personal data they put in the cloud" (AWS, 2018). This means that although AWS will secure its underlying infrastructure, an organization needs to implement their own security practices for protecting their data in the cloud. For example, if an S3 (Simple Storage Service) bucket is created but left open to the internet, AWS cannot be held responsible for the unintentional disclosure of data from the bucket if unauthorized access occurs. This responsibility model reflects the overarching theme of the shift to cloud computing, which is that although there are benefits in terms of cost, security, and flexibility, the CSP is not entirely responsible for managing or securing an enterprise's resources on cloud infrastructure.

Costs in the Cloud

Cloud computing reduces the initial hardware investment of an enterprise's infrastructure, but there are several factors an enterprise must understand to avoid unexpected fees when integrating a cloud service. This includes costs associated with storage, data transfer, and computations made. Without strategies for monitoring cost in the cloud, enterprises can unintentionally encounter unexpected costs. Unexpected cloud computing costs is the most prevalent cause for cloud repatriation, and is typically caused by a lack of cost transparency, or over budgeting the provision of cloud resources (Murugesan, 2024). To ensure that the cost of implementing cloud resources in an enterprise's infrastructure is straightforward, CSPs may provide tools, such as cost calculators, pricing models, and automated billing alerts. These

resources can be utilized by an enterprise to provide clarity in cloud costs. Additionally, cost optimization may be planned in an enterprise's governance framework. Additional costs can also arise from using tools built into a cloud's platform. In the example of AWS GuardDuty, after its free trial, cost is calculated based on the amount per GB of data analyzed, such as AWS CloudTrail events or S3 data events. CloudWatch's free tier allows for 5GB of data ingested per month, charging an additional $0.50 per GB exceeding the free tier, and charging past the creation of 10 metrics alarms. An enterprise can determine if using solutions native to a cloud platform, is suitable for their budget, or if using tools outside of the cloud is more feasible.

Compliance and Regulations

The data an enterprise stores in the cloud may be sensitive, and therefore subject to specific regulations with associated fines for failure to comply with. Common examples of regulations on the storage of sensitive data include the GDPR (General Data Protection Regulation), HIPAA (The Health Insurance Portability and Accountability Act), and PCI DSS (Payment Card Industry Data Security Standard). These three regulations enforce data security requirements for personal data, protected health information, and credit card information, respectively. Other examples of common compliance frameworks include SOC1 for financial auditing, or ISO27001 for security management systems. In the example of AWS, the platform includes AWS Compliance Programs, which provide details on specific resources in AWS to consult in relation to a given framework. In AWS Artifact, enterprises can access related compliance reports and agreements to be accepted for a specific compliance framework (AWS, n.d-a). AWS provides helpful documentation on compliance frameworks, but compliance is the responsibility of the enterprise storing data subject to compliance frameworks on the cloud.

Security in the Cloud

Enterprises will need to adapt to securing their cloud resources based on their CSP's specific platform, which can lead to unintentional misconfigurations. The integration of resources into the cloud requires cloud platform-specific knowledge to successfully mitigate cloud-specific threats. This is due to each platform having its own interpretations of cloud computing terminology for certain processes or resources, which can differ in terminology from on-premise equivalents. Unique cloud terminology can be observed in comparing Identity and Access Management roles in AWS with attached permissions and trust policies, in contrast to an on-premise solution like Active Directory. An enterprise may have a solid security foundation of their on-premise resources, but it is imperative for it to understand their CSP's specific security configuration terminology, and develop a strategy for continuously monitoring the security of their cloud resources.

Unintentional Misconfigurations of Cloud Resources

An enterprise's configuration of cloud resources is unique to their infrastructural needs. Yet, enterprises must maintain a solid understanding of proper cloud configurations needed in order to preserve the security of their infrastructure. According to the Cloud Security Alliance's Top Threats to Cloud Computing 2024 Report, the number one most commonly found threat in 2023 was Misconfiguration and Inadequate Change Control (CSA, 2024). This strongly reflects that enterprises can unintentionally create an insecure cloud infrastructure by not thoroughly ensuring all configurations and changes are managed properly. Common security misconfigurations in the cloud include lack of logging and alerting, access keys being exposed, unsecured databases, lack of network segmentation, and accounts with overly permissive privileges (CSA, 2023). An example of a misconfiguration in the cloud was seen in Accenture's

2017 data breach, when four of their S3 buckets in AWS were configured to allow public access, rather than blocking it. S3 buckets act as a database for files stored in AWS. The buckets were titled with names signifying their importance in Accenture's productions, with terms such as deployment, collector, software, and ssl. The buckets contained sensitive information such as plaintext passwords, VPN keys, access keys, and credentials (UpGuard, 2017). Misconfiguration of cloud resources pose significant risks to an enterprise's continuity of operations, and their reputation if client data stored in the cloud is released.

Identity and Access Management

Identity and Access Management roles being improperly configured was observed in the CSA's Top Threats to Cloud Computing 2024 Report (CSA, 2024). IAM refers to a framework for authenticating users, and assigning them roles with designated permissions for accessing resources. Overly permissive IAM roles provide a user account with higher permissions, such as writing or reading files. When overly permissive roles are granted unnecessarily, they increase an enterprise's attack surface, as the roles can be used as an avenue for privilege escalation. Services or user accounts belonging to a role with heightened permissions are appealing to threat actors, as they provide more access to enterprise resources than roles with more limited privileges. Therefore, it is necessary for an enterprise to appropriately assign IAM roles following the principle of least privilege. A prevalent example of this can be observed from the 2019 Capital One Data Breach, which resulted in the leakage of personal data of about 100 million people in the United States, and about 6 million in Canada. Disclosed data included information from credit card applications, with names, addresses, telephone numbers, email addresses, birthdays, income, linked bank account numbers, and even social security numbers

(Khan et al.,2022). There were several key components that enabled this exfiltration of data from S3 buckets to occur, such as a misconfiguration of the ModSecurity Firewall, and the use of the AWS Instance Metadata service, IMDSV1. However, one of the culprits was the IAM role "IAM-WAF-Role". This role had overly permissive permissions, allowing requests using it to list S3 buckets and download their data (Walikar, 2019). In this data breach, former Amazon employee Paige Thompson was able to obtain a set of AWS access keys from the EC2 metadata service, likely through a Server-Side Request Forgery vulnerability in ModSecurity. AWS has since released a new version of the metadata service, IMDSV2, which prevents SSRF attacks (Walikar, 2019). Even if it was not a misconfiguration of the ModSecurity WAF, the oversight in overly permissive permissions for a role on a public facing server contributed to the execution of the exploit. Data breaches such as these emphasize the importance in maintaining strong security controls and practices for every granular control in an enterprise's infrastructure; no matter how insignificant they may seem.

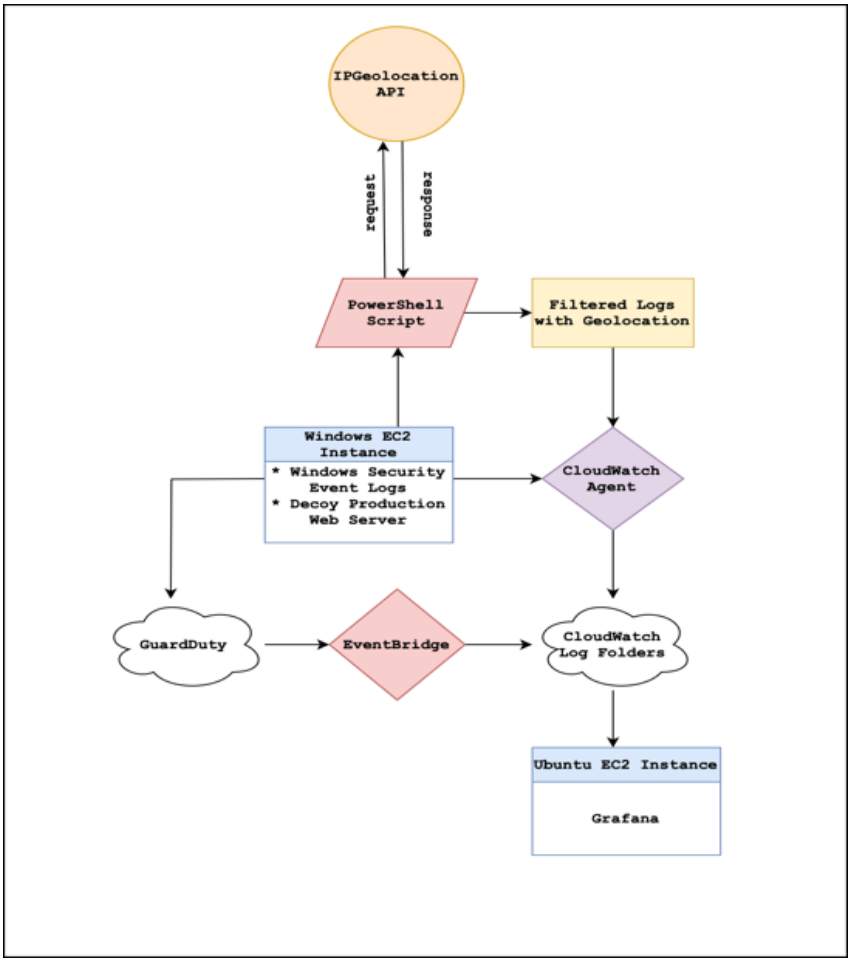
Logging and Threat Detection in AWS

There is always someone looking to exploit cloud resources in the pursuit of financial gain, disruption, or exfiltration of enterprise data. Enterprises must remain vigilant in securing their cloud resources to ensure that they will not fall victim to the disclosure or exfiltration of data stored in the cloud. Amazon Web Services (AWS) is the world's leading cloud service provider, controlling 33% of the cloud market by the end of 2024 (Vailshery, 2025). Their platform provides services to deploy, monitor, and analyze resources in the cloud. Analyzing traffic from services hosted in the cloud has become integrated into the AWS platform, with tools for logging, alerting, and querying security events. An enterprise also has the option of connecting AWS resources for threat hunting or logging to their own third-party tools, such as a

SIEM or SOAR. Following the NSA's recommendations for proper log management, several steps from their guide can be accomplished with AWS: identifying sources for security events is achieved through parsing Windows Security Events from an EC2 instance, collecting and storing logs from selected sources is applied with the configuration of a CloudWatch agent, and analyzing logs with a designated tools is achieved with Grafana.

Figure 1

Flow of Security Event Logs



The Exploitation of AWS EC2 Instances

EC2 instances have several use cases, such as deploying applications, hosting a website, or handling any other compute-heavy task (AWS, n.d-b). When an EC2 instance is left open to all internet traffic, its IP address is able to be found by many worldwide through the use of several tools. Network scanners, such as Nmap, can scan a large network to determine what the available hosts are, what ports are open, and firewall configurations. Another method of discovery could be a website such as Shodan.io, a search engine for internet connected devices which can narrowed down for devices running on the internet with open ports for connection. Misconfiguration of allowed ports and protocols can make enterprise resources more visible, as once a resource in the cloud is connected to the internet and left open to connections from any IP address, there is a higher potential for attempts at reconnaissance.

EC2 Configuration

The instance utilized in this demonstration is a Windows Server 2022 Base, t2.micro instance, with 30 GiB of storage will be used to remain free tier eligible (and due to the small size of the security logs), and is hosted in the region us-east-2. Windows was the chosen operating system, as it enables the use of a PowerShell script for logging Windows Security Events. These events provide security information associated with activities on a Windows machine, such as new logins, or the creation of a new user account, for example. What will make this machine vulnerable is the configuration of its “security group”, an AWS feature for saving specific security configurations. This security group will have no inbound or outbound traffic restrictions on which IP addresses can connect to the instance, and it will not close any ports. Therefore, anyone it is made discoverable to can attempt to connect to it. AWS does warn

against allowing all traffic when configuring security groups, but in this demonstration, a purposeful misconfiguration is made. Additionally, the firewall on the machine has been disabled in the Windows security settings.

The logs gathered from the EC2 instance virtual machine are sent to CloudWatch for further parsing and analysis. To enable this, there are 3 IAM permissions associated: CloudWatchAgentServerPolicy, AmazonEC2RoleForSSM, and CloudWatchLogsFullAccess. Enabling these permissions under a unified IAM role is necessary for the installation and configuration of a CloudWatch Agent on the EC2 virtual machine, otherwise it does not have permission to view and upload the logs. This role must be added to the EC2 instance, under its settings. Additionally, a dedicated policy under another role will be necessary for querying the logs from CloudWatch to Grafana, with "CloudWatchReadOnlyAccess" attached as a permission to read the logs. This role will be attached to another EC2 instance running on Ubuntu, where Grafana is hosted. The infrastructure of AWS heavily relies on permissions for explicitly allowing certain actions. The permissions used may be considered overly permissive due to their ability to read and write security event logs. However, they are being used for the purpose of configuring a vulnerable virtual machine that is not in a real production environment. If an enterprise emulated a similar process for logging, it would need to implement the practice of least privileges when configuring their IAM permissions and roles, strictly maintaining control over which services or user accounts are granted higher permissions.

Hosting a Web Server

Although this machine does not contain any valuable information to an attacker, in order to simulate a common use case of an EC2 instance for an enterprise, a decoy web server is

installed. This could potentially be more enticing to anyone scanning for services running open ports on the internet. The server running is managed by Windows Internet Information Services, and is running on HTTP port 80. If an attacker were to scan the machine for open ports and running services, the server “Production-Env” would appear running on Port 80.

Windows Events and Event Viewer

When certain actions are made on a windows machine, the creation of Windows event log is triggered. There are four categories of Windows Events: System, Application, Security, and Setup. These events are further categorized into severity levels: Information, Warning, Error, and Critical. Each event is assigned a unique number ID in the log. An example of a relevant event for monitoring the vulnerable EC2 instance is Windows Security Event 4625: An account failed to log on. Any event is logged in the Windows Event Viewer, which maintains a record of each event by category, and provides details about the event, such as the timestamp, description, and several more details. With the Windows Event System logging, logs can be extracted for filtering and parsing, internally and externally.

PowerShell Script

Although the CloudWatch Agent uploads all security event logs, they are not structured in an easily readable format, and do not grab geolocation information. Windows PowerShell refers to both a scripting language and command line shell for automating tasks in Windows. Through the execution of a Windows PowerShell script, the log information can be cleanly formatted and provide additional geolocation information of sign on attempts. IPGeoLocation is an API service that can provide geolocation data associated with an IP address. The data utilized with this API are country, city, latitude, longitude, and hostname. The IP address, Windows

Event ID, the timestamp, and the attempted username at sign on are extracted from the information in the Windows Event Log itself. The script parses through recently created Windows Security event logs, filters out these values, and calls the IPGeoLocation API endpoint to log the geolocation data. Each time a new Windows Security Event is found, the relevant information is extracted from it, API endpoint is called, a new jsonl (JSON Line) file is created containing this information. The log files are then uploaded to a designated CloudWatch Log folder, to allow for their analysis in Grafana as dashboard visualizations.

Figure 3

PowerShell Script Gathering Windows Security Event Log Fields and Geolocation Information

```
# PowerShell script to monitor security event logs and fetch geolocation data from IPGeoLocation API service

$directory = "C:\Logs"
$ipGeoKey = "[redacted]"                                    # the API key for IPGeolocation
$lastScriptRun = Get-Date
$sleepSeconds = 5


while ($true) {                                             # Loop to repeatedly check for new security events since the last run of the script
    $currentTime = Get-Date

    try {
        $events = Get-WinEvent -FilterHashtable @{
            LogName = "Security"                            # Windows Security Event Logs
            StartTime = $lastScriptRun
        } -ErrorAction Stop
    } catch {
        Write-Host "Error: $($_.Exception.Message)"         # No new events found
        Start-Sleep -Seconds $sleepSeconds                  # Sleep for 5 seconds before trying again
        continue
    }
        # Extracts the event ID, timestamp, IP address, and username attempted at sign on
    foreach ($event in $events) {
        $xml = [xml]$event.ToXml()
        $eventID = $xml.Event.System.EventID
        $eventTime = $xml.Event.System.TimeCreated.SystemTime
        $username = $xml.Event.EventData.Data | Where-Object { $_.Name -eq "TargetUserName" } | Select-Object -ExpandProperty "#text" -ErrorAction SilentlyContinue
        $ip = $xml.Event.EventData.Data | Where-Object { $_.Name -eq "IpAddress" } | Select-Object -ExpandProperty "#text" -ErrorAction SilentlyContinue
```

```
    # Defining the ipGeo hashtable, which will be filled with geolocation data
    $ipGeo = @{
        country_name = ""
        city = ""
        state = ""
        latitude = ""
        longitude = ""
        hostname = ""
    }
    try {
        $ipGeoURL = "https://api.ipgeolocation.io/ipgeo?apiKey=$($ipGeoKey)&ip=$($ip)" # API endpoint
        $response = Invoke-RestMethod -Uri $ipGeoURL -ErrorAction Stop
        $ipGeo.country_name = $response.country_name
        $ipGeo.city = $response.city
        $ipGeo.state = $response.state_prov
        $ipGeo.latitude = $response.latitude
        $ipGeo.longitude = $response.longitude
        $ipGeo.hostname = $response.hostname
    } catch {
        Write-Host "Did not get geolocation info for: $ip - $($_.Exception.Message)"              # If there is an error reaching IPGeolocation API endpoint, print exception message
    }
    # Updating the log information
    $logEntry = @{
        timestamp = $eventTime
        event_id = "$eventID"
        user = $username
        ip = $ip
        ipGeo = $ipGeo
    }

    # Writes a new json log file for each API call, with the file name set to the event ID + timestamp
    $json = $logEntry | ConvertTo-Json -Depth 5 -Compress
    $time = (Get-Date $eventTime -Format "yyyyMMdd_HHmm")
    $fileName = "event_${time}_ID${eventID}.json1"
    $filePath = Join-Path $directory $fileName
    Set-Content -Path $filePath -Value $json
    Write-Host (Get-Content -Path $filePath -Raw)   # Print the file contents to the PowerShell
}

$lastScriptRun = $currentTime                      # Update the most recent run time
Start-Sleep -Seconds $sleepSeconds                 # Sleep for 5 seconds before running again
}
```

AWS CloudWatch

The centralization of logs is needed in case the EC2 instance becomes compromised, and access to the logs on the machine is disrupted or lost. CloudWatch can be configured to monitor and transport both custom logs and regular Windows Event Security Logs. Logs that exist on the instance can be uploaded to the cloud, with the installation of a CloudWatch Agent. In this configuration, a CloudWatch Agent monitors new logs in two locations: the Windows Event viewer, and a folder labeled “Logs”. The “Logs” folder is the designated directory that the PowerShell script will output filtered logs to. Furthermore, CloudWatch metrics allow for monitoring performance metrics of EC2 instances, such as CPU utilization, and bytes traveling in and out of its network. Custom metrics can be created for implementing alerting based on EC2 instance logs. Once an alert is created, an action such as a function being triggered with AWS Lambda, an email, or an SMS text message can be sent if a log matches the alert. CloudWatch has also had Machine Learning elements, with the integration of Log Anomalies, and AWS

"Detective", two services leveraging AI for log analysis. Alerting and machine learning for logging are notable features of AWS, but were not selected in the analysis of failed sign in logs, since all of the logs match the same Windows Security Event ID: 4625.

Figure 5
CloudWatch Agent Configuration

```
"logs": {
        "logs_collected": {
                "files": {
                        "collect_list": [
                                {
                                        "file_path": "C:\\Logs\\*",
                                        "log_group_class": "STANDARD",
                                        "log_group_name": "custom_logs",
                                        "log_stream_name": "{instance_id}",
                                        "retention_in_days": 30
                                }
                        ]
                },
                "windows_events": {
                        "collect_list": [
                                {
                                        "event_format": "xml",
                                        "event_levels": [
                                                "WARNING",
                                                "ERROR",
                                                "CRITICAL",
                                                "INFORMATION"
                                        ],
                                        "event_name": "Security",
                                        "log_group_class": "STANDARD",
                                        "log_group_name": "windows-security-events",
                                        "log_stream_name": "{instance_id}",
                                        "retention_in_days": 30
                                }
                        ]
                }
        }
}
```

GuardDuty in AWS is a threat detection tool that can be enabled for an EC2 instance to observe abnormal behavior. It utilizes threat intelligence feeds for determining if there is malicious activity associated with the instance, producing alerts on port scanning, malware detection, or any other unusual activity. As mentioned, an EC2 instance exposed to the internet can be found by attackers through port or network scanning, and dedicated search engines. Therefore, the specific event to be monitored from GuardDuty is associated with reconnaissance: EC2/PortProbeUnprotectedPort. This finding detects when a port is being probed on an EC2 instance by a malicious host machine. Since the ports 22 and 3389 are left open for any host to attempt connection to, if these ports are or any others are probed, a log will be generated in

GuardDuty. Logs for this alert automatically grab geolocation data for associated IP addresses performing scans on an instance, and can be exported to CloudWatch logs for visualizations in Grafana.

Grafana

Tools for creating visualizations are commonly utilized in network infrastructures to provide insights into network traffic. Examples of these include Kibana, Splunk, and Grafana. AWS has resources for creating visualizations, such as in CloudWatch (with costs associated after the creation of three dashboards), however it also supports integrations for third-party visualization tools. These integration capabilities allow for more flexibility and cost optimization when integrating cloud resources, as enterprises have expanded options beyond tools native to their cloud platform. Grafana is an open-source tool for creating dashboards, and includes a database connection feature with AWS CloudWatch. Enabling this connection allows a log folder to be queried with SQL (Structured Query Language), for creating visualizations and dashboards. By querying the log data by specific fields, such as the location of an IP address or port probed, visualized insights into sign in attempts on the open EC2 instance can be created. Although Grafana can be hosted outside of the cloud, this installation of Grafana is hosted on an Ubuntu EC2 instance. It has not been made open to the internet, and can only be accessed on port 3000 once a connection over SSH is established from my local machine.

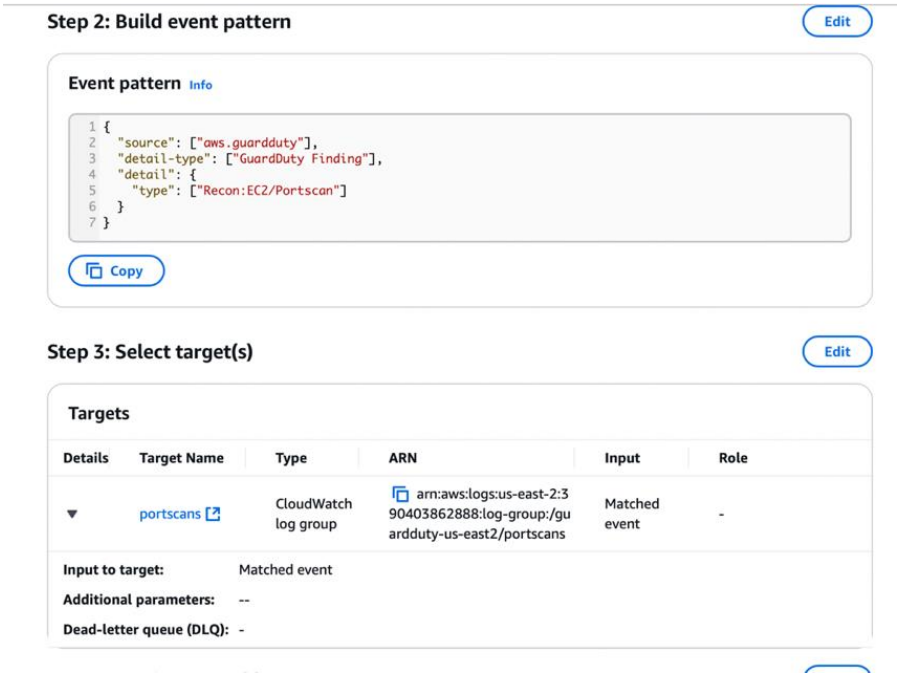
Event Bridge

The results from GuardDuty regarding port scanning do not import into CloudWatch natively, and therefore must configured in order to be queried in Grafana for creating visualizations. This can be accomplished with the creation of an Event Bridge rule, with an event

pattern matching "Recon:EC2/Portscan" from GuardDuty, and a target set to a specified log group in CloudWatch to store the JSONs matching this pattern. Once the rule is configured, any new port scans detected by GuardDuty will be exported to the CloudWatch log group. EventBridge could also be utilized by an enterprise for automating the response to security events, as it can match a pattern from logs in CloudWatch, and trigger any desired reaction to logs matching that pattern.

Figure 6

Event Pattern and Selected Target for AWS EventBridge



Running the Script and Log Analysis

Once the EC2 instance is up and the script is run with PowerShell, login attempts can be observed shortly after. These attempts typically occur in quick succession, and persist for varying amounts of time. The behaviors of the sign on attempts suggest that an automated process such as a script has been created for finding open machines on the internet, and attempting a combination of many different usernames to gain remote access.

Figure 7

Sign in attempts from PowerShell Command Line Shell

As discussed, each attempt generates a new log file stored in a folder on the machine, which is then uploaded to CloudWatch. The CloudWatch logs contain the same information from the PowerShell Command line shell, but the Guard Duty event logs for port probing contain additional fields for the port and port name.

Figure 8

A GuardDuty Event Log


```
{
    "CreatedAt": "2025-04-17T13:48:49.235Z",
    "InstanceId": "i-01a678ff00dcac65d",
    "PublicIp": "3.145.168.222",
    "RemoteIp": "198.251.88.248",
    "RemoteCountry": "Luxembourg",
    "RemoteCity": "Luxembourg",
    "RemoteLat": 49.6113,
    "RemoteLon": 6.1294,
    "RemoteASN": "53667",
    "RemoteOrg": "FranTech Solutions",
    "RemoteIsp": "FranTech Solutions",
    "Port": 445,
    "PortName": "SMB",
    "Title": "An unprotected port on EC2 instance i-01a678ff00dcac65d is being probed.",
    "ThreatList": "ProofPoint"
}
```


Upon comparing the log results from the CloudWatch Agent to the GuardDuty logs, a few observations can be made. The found probed ports were 445, 5985, 135, and 47001. Port 445 is used by several Windows services, such as Active Directory, or Server Message Block for file sharing. Port 5985 is used by Windows Remote Management, for HTTP connections. Port

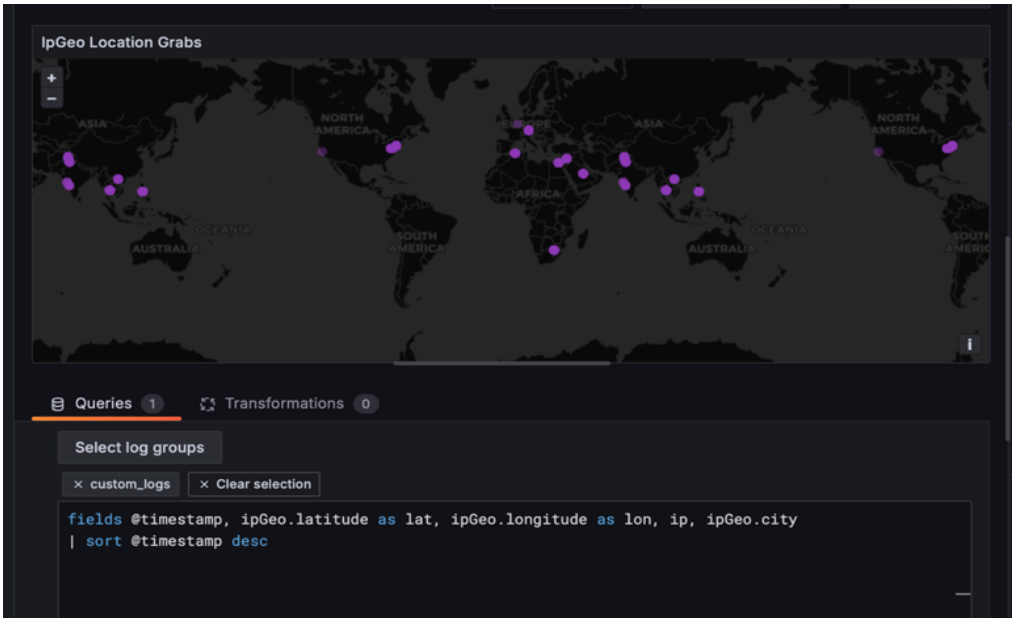
135 is used by the RPC Endpoint Mapper, which allows for discovery on which services are running on certain ports. The final observed port was 47001, Windows Remote Management, for HTTPS connections. These ports are targeted as they are either be running insecure protocols such as SMB, or can provide additional information on a machine about services running, the operating system it has. Another observation is that there is not an equal volume of detected port scans to IP addresses attempting to connect to the machine, with the logs having over 20,000 sign in attempts, but GuardDuty only catching 27 occurrences of port scanning. Some countries associated with the port scans, such as Luxembourg in Figure 8, were not observed in the failed remote sign on logs. This signifies that further methods of location obfuscation may be in place from the machines attempting to sign into the instance, such as a VPN or proxy servers.

Grafana Dashboards

The chosen visualizations created for the logs include a table of sorted attempted usernames, a table of sorted IP Addresses observed, a table of scanned ports, and a global map of sign in attempts. Each visualization is created with tailored queries to a specific log group stream in CloudWatch.

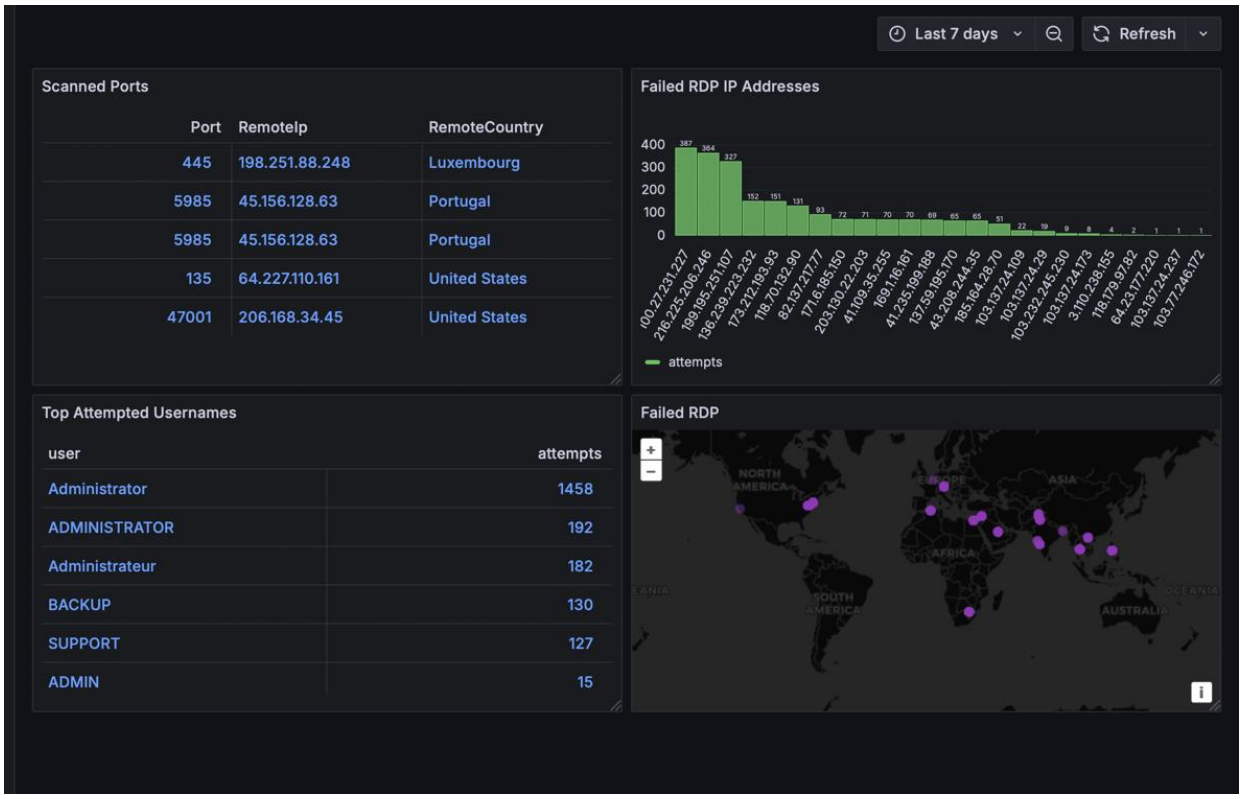
Figure 9

Query to create GeoMap for EC2 instance



Collectively, these individual visualizations can be added to a single dashboard:

Figure 10
Grafana Dashboard for EC2 Instance



Conclusion

There are many opportunities for growth of an enterprise wanting to integrate their infrastructure into the cloud, as the cloud can reduce costly hardware investments. However, there is also complexity associated in several areas of shifting to the cloud, as seen across cost transparency, meeting compliance, and in security, with unintentional security misconfigurations. It would be beneficial to an enterprise looking to migrate into the cloud to conduct thorough research on establishing a cloud governance framework to follow. It is also necessary to maintain an understanding of how the cloud will affect their needs for cost efficiency and compliance requirements, and to ensure that they can adapt to cloud specific

security concepts, so as to not experience unintentional misconfigurations when making the transition. These misconfigurations can lead to the enterprise becoming a target of an APT group targeting unsecured resources in the cloud.

AWS tools for threat detection and logging, of which can be integrated into third party services, are capable of providing meaningful insights into cloud resources, including ones that has been misconfigured as with the EC2 instance. AWS has several services dedicated to the logging and monitoring of resources on the cloud, as observed with CloudWatch logs and metrics, GuardDuty, and EventBridge. However, cloud costs can be increased through utilizing additional features such as these. If an enterprise prefers tools native to AWS for logging or threat detection, it should carefully monitor how these tools fit into their cloud budget. Ultimately, it is up to an enterprise to discern if additional useful tools in their CSP's platform can meet their infrastructural and cost management needs. This consideration further contributes to the complexities enterprises face when shifting to the cloud.

References

Alvarenga, G. (2023). *What is cloud governance? building the framework*. CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-governance/

AWS. (n.d.-a). *What is AWS artifact?* https://docs.aws.amazon.com/artifact/latest/ug/what-is-aws-artifact.html

AWS. (n.d.-b). What *is Amazon EC2? - Amazon elastic compute cloud*. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html

Cloud Security Alliance (CSA). (2024). *Top threats to cloud computing: The notorious eleven.* https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024

Cloud Security Alliance (CSA). (2023). *Cloud Misconfigurations That Lead to Data Breaches*. https://cloudsecurityalliance.org/blog/2023/10/11/the-common-cloud-misconfigurations-that-lead-to-cloud-data-breaches

Cloud Security Alliance (CSA) (2025). *How can businesses Secure Hybrid Cloud Environments?* https://cloudsecurityalliance.org/blog/2025/03/27/hybrid-cloud-security-top-challenges-and-best-practices

CrowdStrike (2025). *2025 threat hunting report*. https://www.crowdstrike.com/en-us/global-threat-report/

Flinders, M., & Smalley, I. (2024). *What is xaas (anything as a service)?*. IBM. https://www.ibm.com/think/topics/xaas

Khan, S., Kabanov, I., Hua, Y., & Madnick, S. E. (2022). *A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned*. ResearchGate. https://www.researchgate.net/publication/361860348_A_Systematic_Analysis_of_the_Capital_One_Data_Breach_Critical_Lessons_Learned

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

National Security Agency (NSA). (2024). *Manage logs for effective threat hunting*. National Security Agency. https://media.defense.gov/2024/Mar/07/2003407864/-1/-1/0/CSI_CloudTop10-Logs-for-Effective-Threat-Hunting.PDF

Shirer, M. (2024). *Worldwide Spending on Public Cloud Services is Forecast to Double Between 2024 and 2028, According to New IDC Spending Guide.* IDC: The Premier Global Market Intelligence Company. https://www.idc.com/getdoc.jsp?containerId=prUS52460024

Susnjara, S. (2024). *Private cloud examples, applications & use cases*. IBM. https://www.ibm.com/think/topics/private-cloud-examples

Walikar, R. (2019). *An SSRF, privileged AWS keys and the capital one breach*. Medium. https://blog.appsecco.com/an-ssrf-privileged-aws-keys-and-the-capital-one-breach-4c3c2cded3af

SpiceWorks (2025). *What is platform as a Service (paas)? definition, examples, components, and best practice*s. https://www.spiceworks.com/tech/cloud/articles/what-is-platform-as-a-service/

UpGuard (2017). *System shock: How a cloud leak exposed Accenture's business*. https://www.upguard.com/breaches/cloud-leak-accenture

Vailshery, L. S. (2023). *Global cloud infrastructure market share by vendor 2017-2019.* Statista. https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/

Zgola, M. (2024, August 13). *The Rise of Cloud Repatriation: Why Companies are bringing data in-house*. Forbes. https://www.forbes.com/councils/forbestechcouncil/2023/04/18/the-rise-of-cloud-repatriation-why-companies-are-bringing-data-in-house/