C.S.S.A TECH

RoadMap Cloud Security 2022

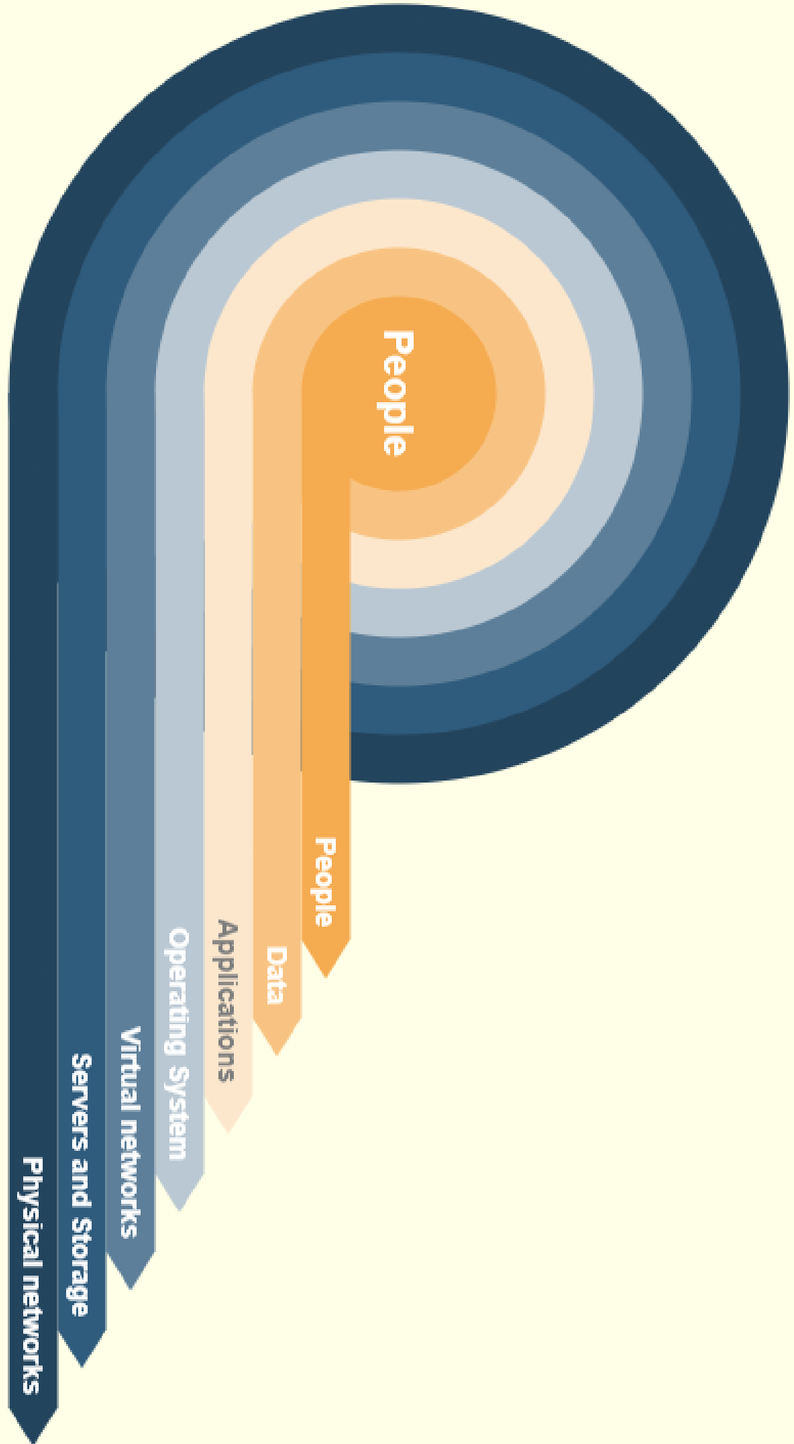
Version 1

C.S.S.A Guide V. 1 | 2022

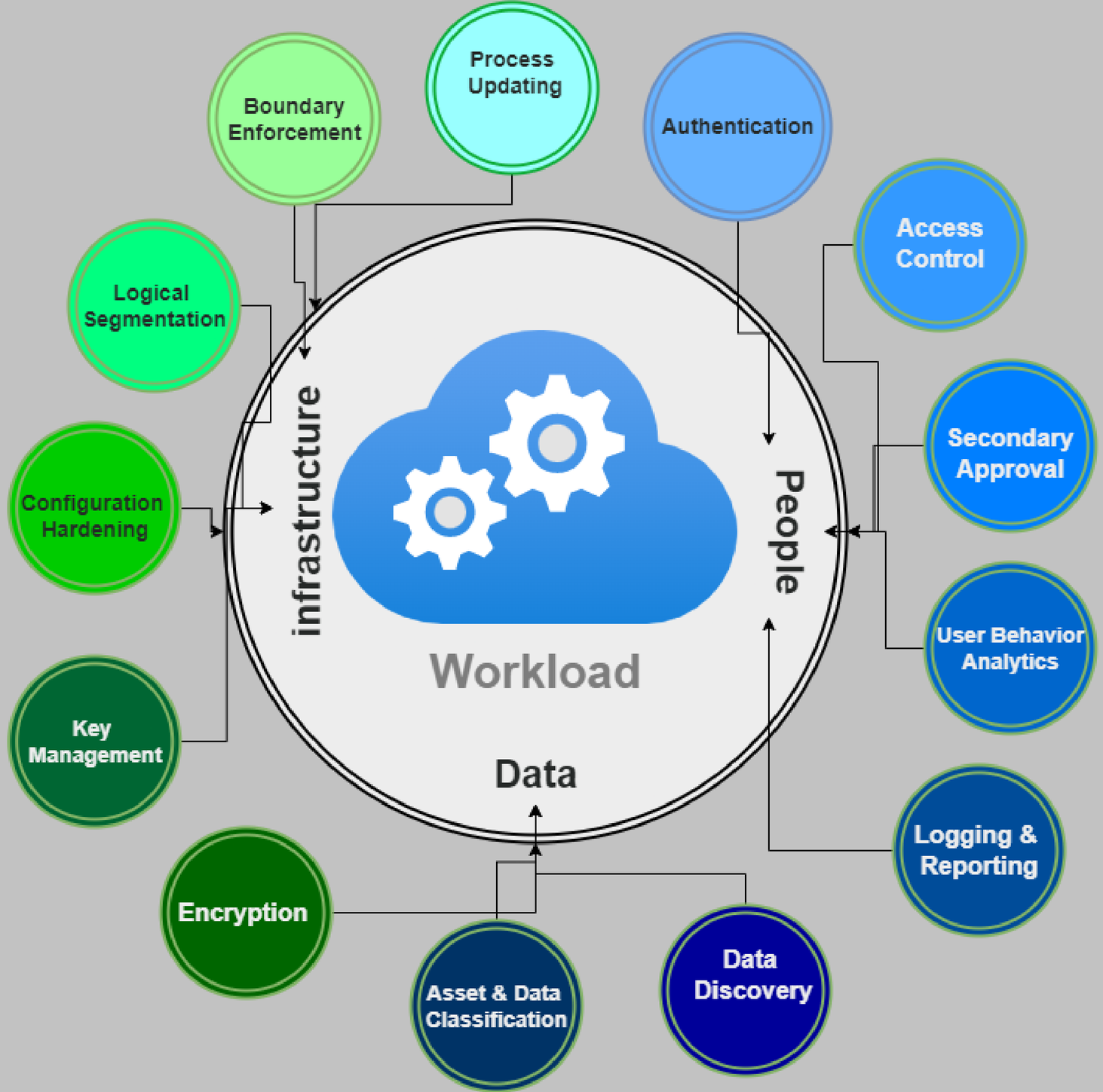
Cloud security is about protecting your cloud-based systems, data, and infrastructure from threats.

Cloud computing offers several advantages over traditional on-premise datacenters: it's easier to scale up and down as needed; it's easy to collaborate with others in real time; and it can be hosted far away from your organization's headquarters.

But the fact that these advantages exist only because of a cloud infrastructure makes them vulnerable to attack. The best way to protect against this is through an integrated approach that includes technologies, controls, processes, and policies.



MODEL FOR SECURING CLOUD WORKLOADS



Set Strategies and Tools

1- Identity and Access Management

IAM is a way to control access to your applications and data. It's a system that allows you to control who has access to your applications, what they can access, and what they can do to your data.

2- Physical Security

In order to ensure physical security for your data, you should ensure that the following measures are in place:

-Regular user scans for malware and other threats

-Regular updates of software and patches on all systems

-Regular backups of data and systems

3-Threat Intelligence, Monitoring, and Prevention

Threat intelligence, intrusion detection systems (IDS), and intrusion prevention systems (IPS) form the backbone of cloud security. On-premise IDS tools deliver functionality to identify attackers who are currently targeting your systems or will be a future threat. On-premise IPS tools implement functionality to mitigate an attack and alert you to its occurrence so you can also respond.

Many companies use these three security tools together to create a comprehensive security solution that protects against the most sophisticated attacks.

Set Strategies and Tools

4- Encryption

Encryption is one of the most important layers of cloud security. It allows you to send and receive data from the cloud provider's platform, and it also ensures that your data is protected when it's not in use. Encrypting your data at rest and in transit ensures that it's impossible to decipher without an encryption key that only you know about.

5- Micro-Segmentation

Micro-segmentation is a way to deploy cloud security that is increasingly common. It's the practice of dividing your cloud deployment into distinct security segments, right down to the individual workload level.

By isolating individual workloads, you can apply flexible security policies to minimize any damage an attacker could cause, should they gain access.

6- Cloud Vulnerability and Penetration Testing

Cloud security is a bit of a minefield. There's no shortage of ways to hack into a cloud infrastructure, and the best way to protect yourself from these risks is to ensure that you're doing everything possible to defend against them.

One key practice that you can implement is vulnerability and penetration testing. This involves your provider or yourself attacking your own cloud infrastructure in order to identify any potential weaknesses or exploits. Once you've identified all the potential vulnerabilities, you can then implement solutions to patch them and improve your security stance.

Next-Generation Firewalls

Next-generation firewalls are another piece of the cloud security puzzle. They protect your workloads using traditional firewall functionality and newer advanced features. Traditional firewall protection includes packet filtering, stateful inspection, proxying, IP blocking, domain name blocking, and port blocking.

Next-generation firewalls add in an intrusion prevention system, deep packet inspection, application control, and analysis of encrypted traffic to provide comprehensive threat detection and prevention.

The combination of these features means that you can give your users a better experience when accessing sensitive data from any location.

Security Risks of Cloud Computing

Whether you're running in the cloud or not, security is an important concern for every business. You'll face risks such as denial of service, malware, SQL injection, data breaches and data loss. All of which can significantly impact your reputation and bottom line.

When you move to the cloud, you introduce a new set of risks—and change the nature of others. That doesn't mean cloud computing isn't secure. In fact, many cloud providers introduce access to highly sophisticated security tools and resources you couldn't otherwise access.

It simply means you need to be aware of the change in risks in order to mitigate them. So let's take a look at some unique security risks of cloud computing:

Insecure Application User Interface (API)

When operating systems in a cloud infrastructure, you might use an API to implement control. Any API built into your web or mobile applications can offer access internally by staff or externally by consumers.
It is external-facing APIs that can introduce a cloud security risk. Any insecure external API is a gateway offering unauthorized access by cybercriminals looking to steal data and manipulate services.

Lack of Cloud Security Strategy and Architecture

Many organizations are taking advantage of the cloud by migrating systems and data to the cloud, but they often become operational long before the security systems and strategies are in place to protect their infrastructure.
The result is a lack of cloud security that can leave companies vulnerable to attacks. The good news is that you can easily avoid this risk by setting up a cloud security strategy and architecture right from the start.

Contractual Breaches

The use of shared data is a key part of any business partnership, and it's essential that you protect that data from any breaches.
If your employee unwittingly moves restricted data into a cloud service without authorization, it could create a breach of contract which could lead to legal action.

Loss of Visibility

You can lose visibility of who has access to your cloud services, what data they are accessing, uploading, and downloading. If you don't know who is using your cloud resources – and why – you can't protect them or prevent someone else from doing so.

Insider Threats

Insider threats are a real problem for many companies. These aren't just the malicious actors in hacking, or even the people who do it on purpose. Instead, they are your trusted employees, contractors, and business partners who can cause major damage to your business.

Misconfiguration of Cloud Services

Misconfigured cloud services are often caused by default settings that allow sensitive data to be publicly exposed or manipulated.
Mismatched access management can also lead to unauthorized individuals gaining access to confidential data. When these things happen, your company's reputation is on the line—and it could mean losing customers in the long run.

Compliance Violations

There are many regulations that require your company to know where its data is, who has access to it, how it is processed and how it is protected. Another regulation requires that your cloud provider holds certain compliance credentials.

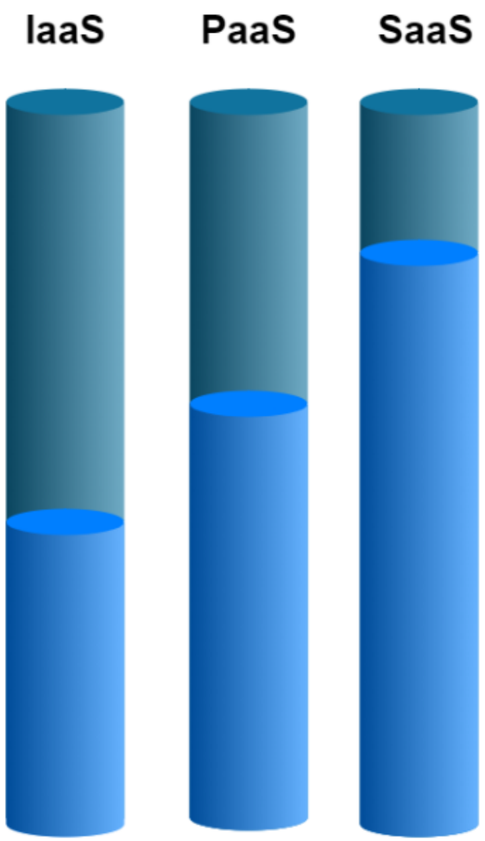
Why Cloud Security is Required

- Cyber Security Threats Continue to Increase
- Preventing Data Breaches and Data Loss
- Maintaining Business Continuity
- Avoid Compliance Violations

Cloud Security Benefits

- Centralized Security
- Reduced Administration
- Increased Reliability
- Reduced Cost

Understand Your Shared Responsibility Model

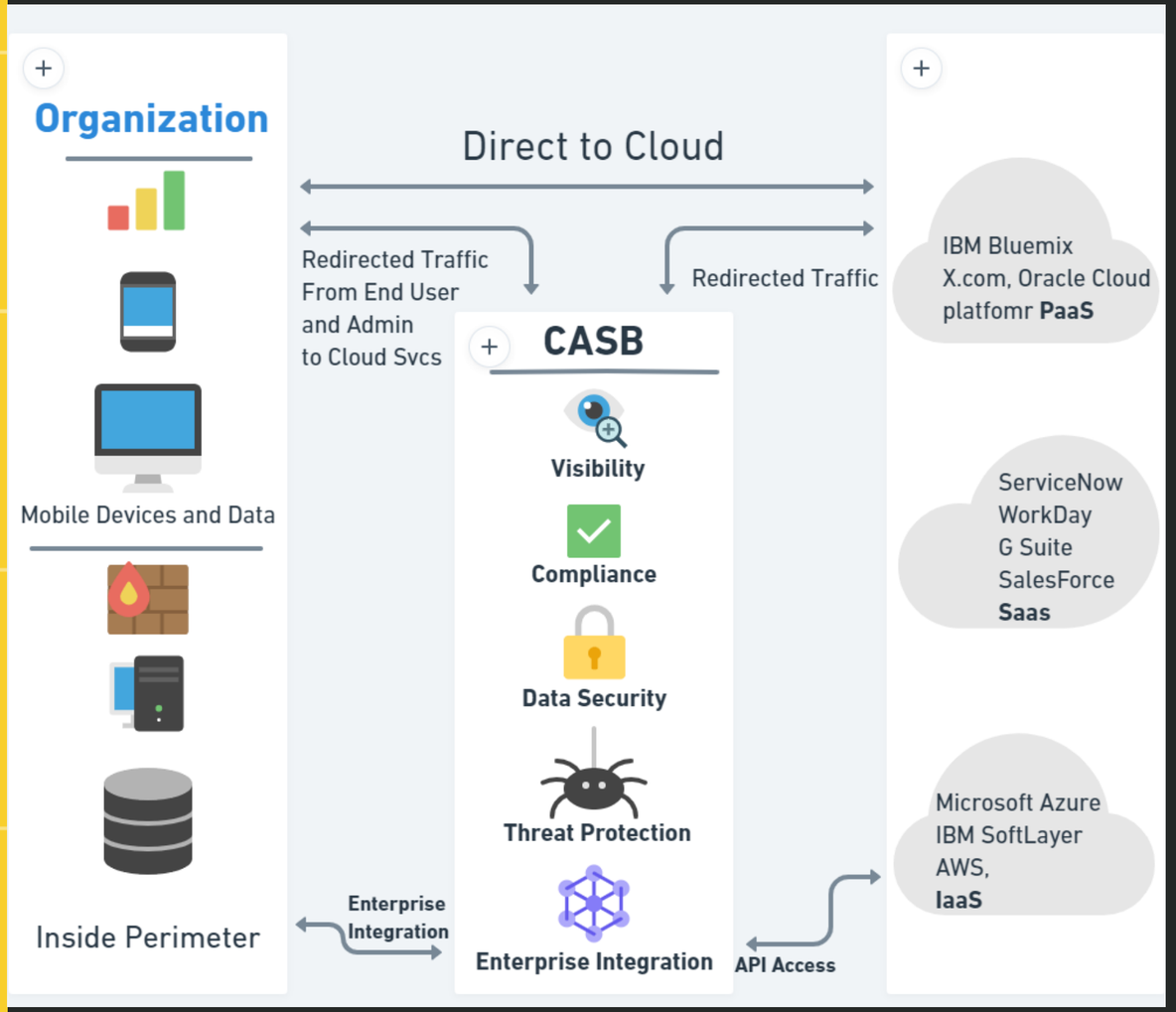


Implement a Strong Password Security Policy

Control User Access

Secure Your User Endpoints

Train Your Users



CASBs are the perfect solution for you if you're looking for a way to protect your organization from cyberattacks and keep your data safe.

A CASB will help you defend against high-level cloud security risks, as well as support ongoing monitoring and mitigation of high-risk events. It does this by securing the data moving between your on-premise and cloud environment using your organization's security policies.

A CASB will protect you from cyberattacks with malware prevention and secure your data using end-to-end encryption preventing outside users from deciphering the content. Plus, it can provide additional security measures such as deep packet inspection for additional protection against malicious attacks.

How does a CASB work?

A CASB can be deployed in three separate ways: as a reverse proxy, forward proxy, or in an 'API mode'. Each has its own unique advantages and disadvantages, with many industry experts recommending a multimode deployment.

Reverse Proxy

A reverse proxy sits in front of the cloud service, providing inline security capabilities by sitting in the path of the network traffic.

The connection of the reverse proxy broker runs from the internet to your application server, hiding information behind it that is coming from the original source.

This can be used to provide arbitrary origin protection or to enforce strict security requirements, such as requiring SSL/TLS for all requests.

Forward Proxy

A forward proxy sits in front of the user, with the CASB proxying traffic to multiple cloud platforms. The connection of the forward proxy runs from you, sat behind your firewall, to the internet. Like the reverse proxy, it also provides inline security capabilities.

Like a reverse proxy, a forward proxy can be used to support multiple protocols or applications (e.g., HTTP and HTTPS). But unlike a reverse proxy, it can also function as a load balancer between multiple cloud platforms (e.g., Amazon Web Services and Microsoft Azure).

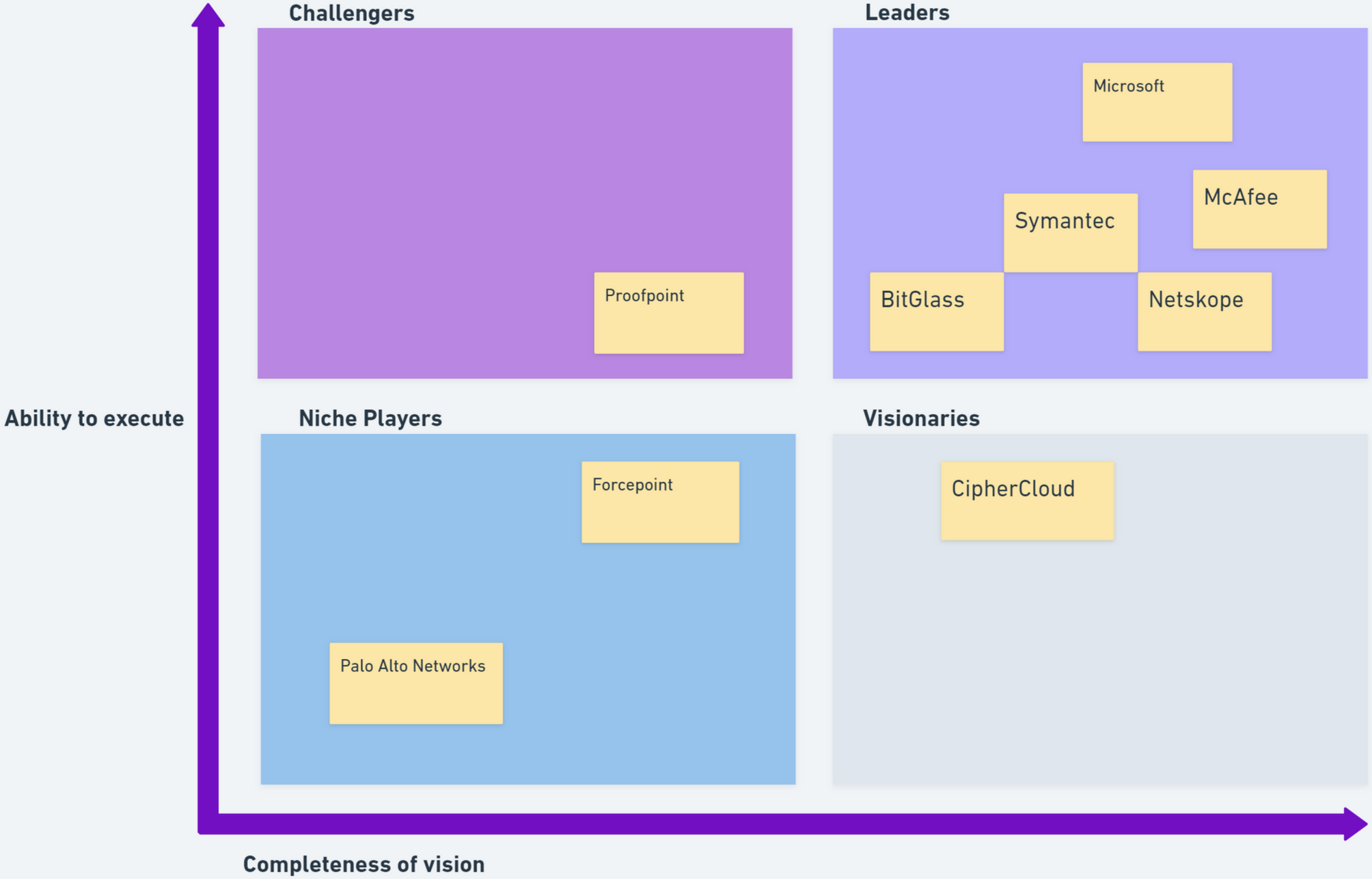
API Mode

The Application Program Interface (API) is one of the most popular ways to integrate CASB and cloud services. Using an API allows for direct integration of the CASB and a cloud service.

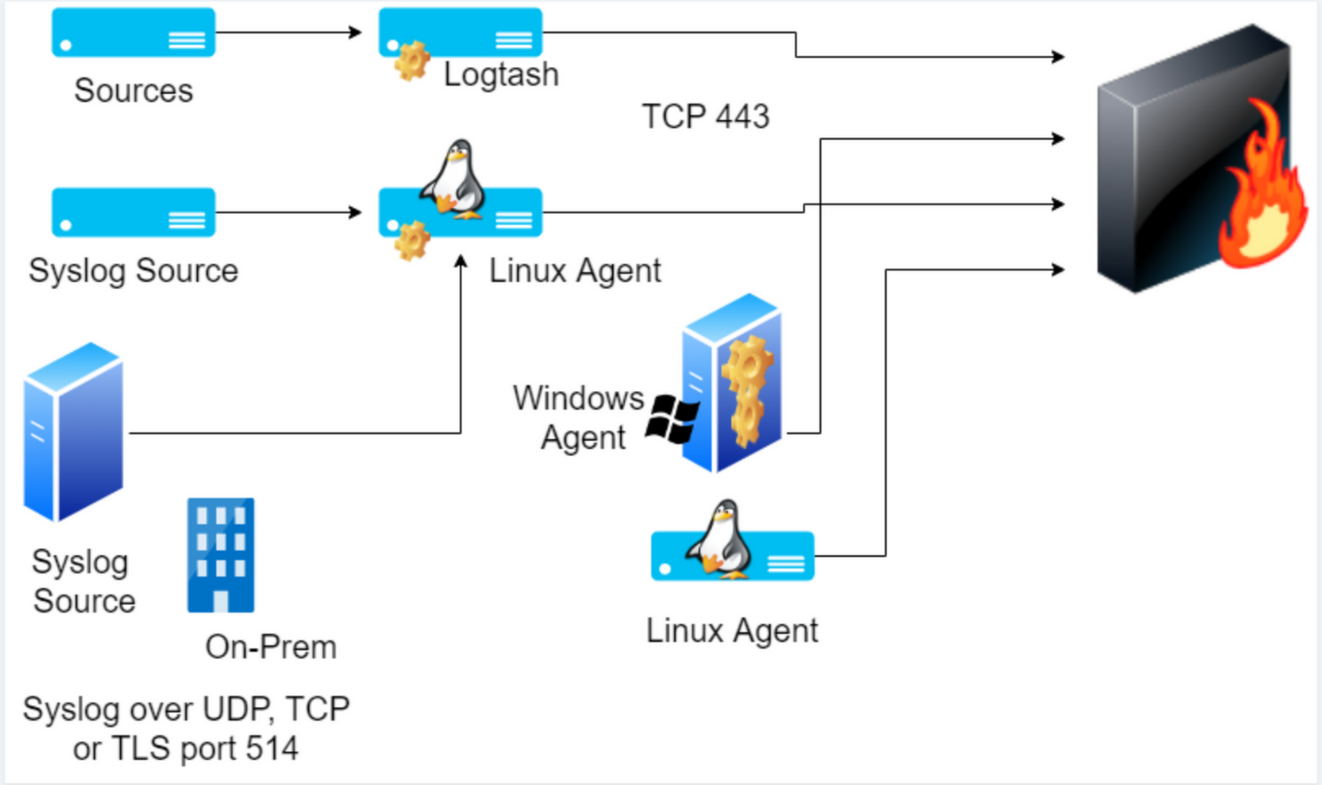
This allows you to secure both managed and unmanaged traffic. Depending on the cloud service providers' API functionality, you can view activity, content, and take enforcement action.

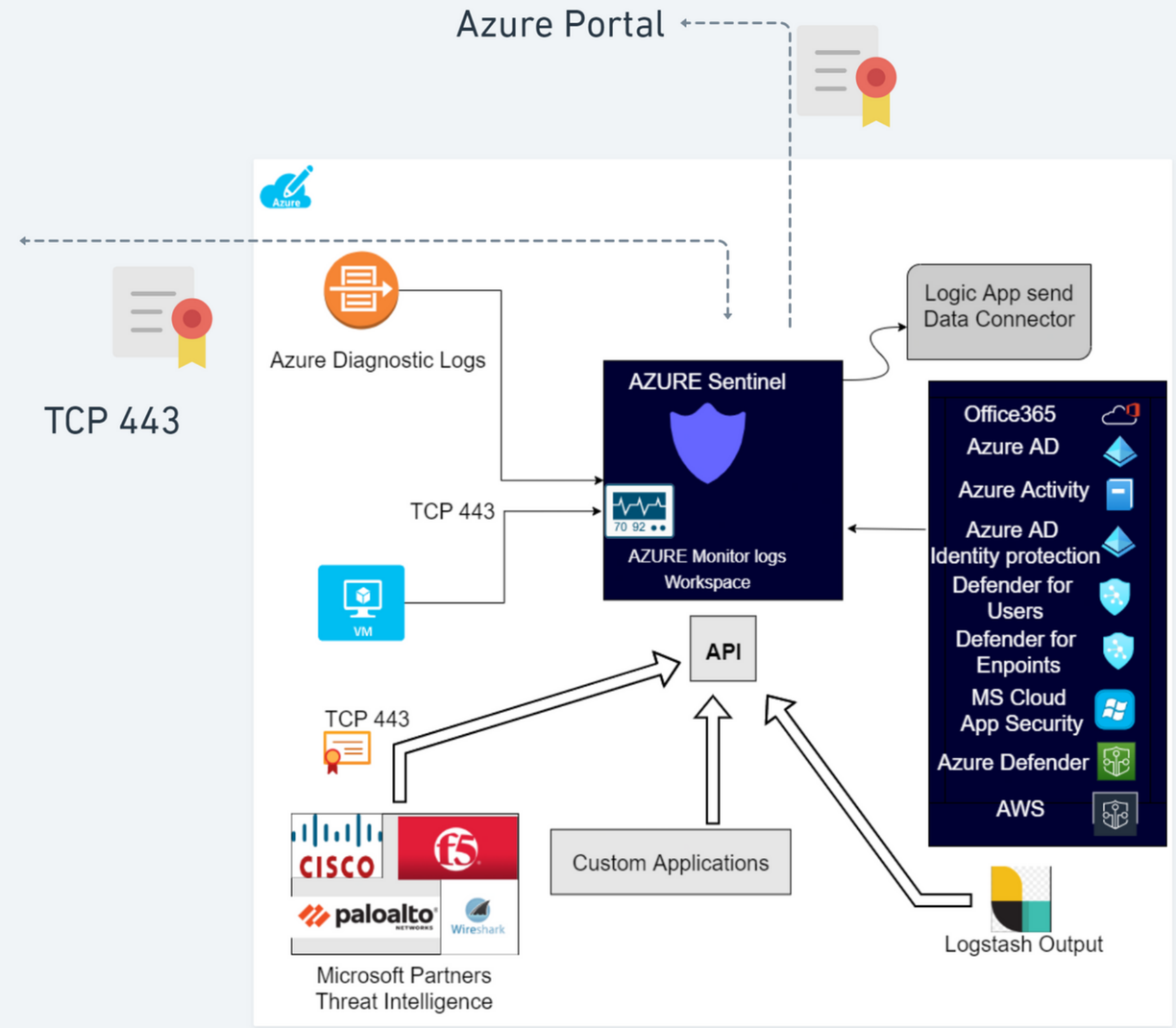
1. Visibility
2. Data Security
4. Compliance
3. Threat Protection

Cloud Access Security Broker (CASB)



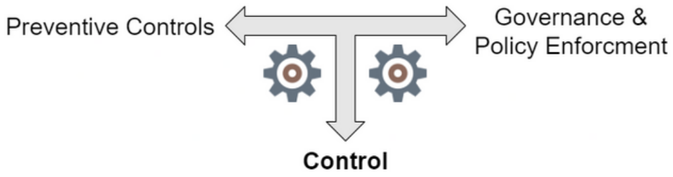
Data Ingestion Architecture

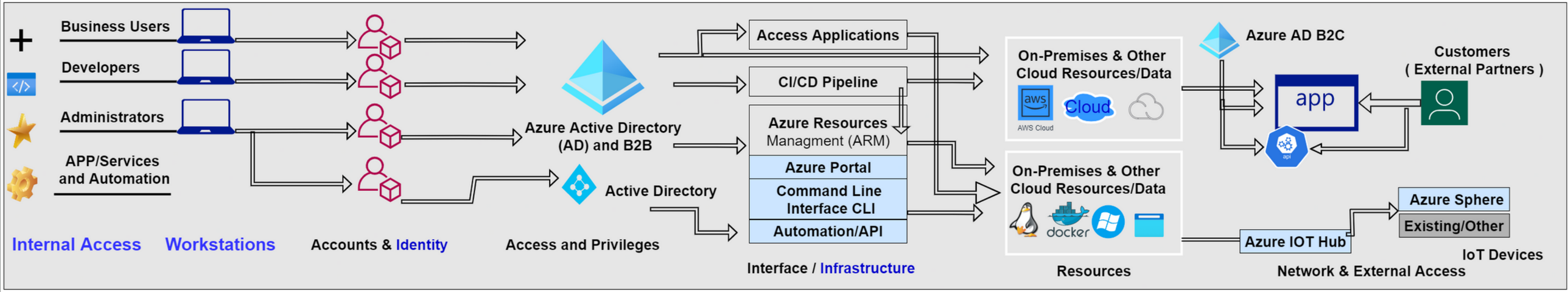


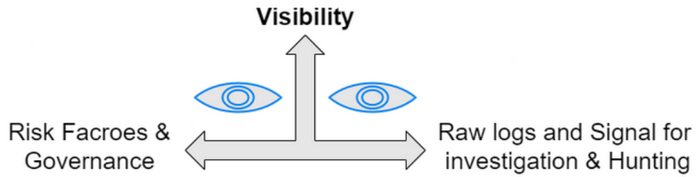


Zero Trust Principles

End to end capabilities that apply ZeroTrust principles infrastructure (IaaS & Paas)







C.S.S.A Guide V. 1 | 2022

RoadMap Cloud Security 2022

This RoadMap get's updated every 8 weeks based on latet's security risk.

Mitre ATT&CK

OWASP