

**Cloud Security & Management Lab**

**Submitted by**

**Name – Shiva Shukla**

**SAP ID – 500084634**

**Roll no – R2142201078**

**Batch – B1**

**Program – B.Tech CSE spl CCVT**

**Submitted**

**“ Ms. Amanjot Kaur” Mam**

**Cloud Security Tools with working principles, advantages, disadvantages, limitations, applications**

1. **Cato Networks**

The SASE tool from Cato is a cloud-based security product that combines SD-WAN, network security, and compatibility for a range of mobile devices and cloud applications.

**Working** : Customers make use of Internet services provided by third parties. A physical device (the Cato Socket) or a virtual appliance can connect two locations (the vSocket). Connecting to Cato's mobile client on a mobile device (the Cato Client). To reach the nearest PoP, each Cato node creates a safe tunnel across the Internet connection.

**Advantages:**

* Migration of MPLS to Secure SD-WAN.
* remote access security
* Internet access for secure branches.
* Global Connectivity optimised.
* Multi-Cloud and Hybrid Cloud Security.
* Working at home.

**Disadvantages:** Cato Networks does its intended tasks and even goes beyond its capacity when delivering additional features.

**Limitations:** not receiving emails for scheduled reports.

**Applications:**

Data Loss Prevention (DLP), SD-WAN as a Service, Cloud Access Security Broker (CASB), Security Service Edge (SSE), and Zero Trust Network Access (ZTNA).

Alternatives Worldwide to MPLS.

UCaaS optimization and UC.

1. **Fugue**

Engineers created the cloud-based, enterprise-focused CSPM product Fugue to provide comprehensive visibility into a company's security posture. Fugue has a strong emphasis on upholding compliance rules and offers an API for simple implementation.

**Working:** The subject of a fugue is introduced in one of the voices by itself in the tonic key. After the topic is stated, the answer is delivered by a second voice that transposes the subject to a different key (often the dominant or subdominant).

**Advantages:**

Addresses differences in behaviour across various compute frameworks (Pandas, Spark, and Dask)

enables code reuse for data of both Pandas- and Spark-sized.

greatly reduces project costs overall and dramatically accelerates testing.

allows for considerably faster productivity with Spark for novice users.

**Disadvantages :** The general input I have is that there is an opportunity for them to better align with other similar tools and better align with similar capabilities that cloud suppliers deliver natively.

**Limitations :** For vocal fugues, the compass is often within an octave.

**Applications** :

A fugue usually has three main sections: an exposition, a development and a final entry that contains the return of the subject in the fugue's tonic key.

1. **Firewalls**

Firewalls are security tools that regulate traffic entering and leaving a network. Incoming traffic is compared to a set of predetermined rules, and only traffic that complies with those standards is permitted to pass through.

**Advantages:**

Firewalls can be used to apply least privilege principles, regulate access to resources, and provide a minimum level of security for cloud settings.

**Disadvantages:**

Firewalls must be properly configured and maintained in order to function correctly in high-throughput environments.

**Limitations:** A firewall can only defend against known threats, and attackers who employ techniques like packet fragmentation or encryption can get around it.

**Applications:** Firewalls are frequently used in cloud environments to impose least privilege and restrict access to resources.

1. **Virtual Private Network (VPNs)**

A VPN is a piece of technology that establishes a secure link between two networks, such as the on-premises network of a business and the cloud. It functions by encrypting all data delivered over the connection, which makes it more challenging for unauthorised parties to access the data.

**Advantages:**VPNs give networks a secure connection, making it more challenging for unauthorised users to access data.

**Disadvantages:**VPNs can be difficult to set up and manage, and they can also increase latency and decrease performance.

**Limitations:** Because VPNs rely on the security of the underlying network, they will not be secure if the underlying network is unsecure.

**Applications:** To provide secure connections between on-premises systems and cloud environments, VPNs are frequently employed.

### [Security code scan](https://github.com/security-code-scan/security-code-scan)

* This open source tool detects various security vulnerability patterns like SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), XML external Entity Injection (XXE), etc.

**Working** : Detects various security vulnerability patterns: SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), XML eXternal Entity Injection (XXE), etc. Inter-procedural taint analysis for input data. Continuous Integration (CI) support for GitHub and GitLab pipelines.

**Advantages :** Code scanning enables vulnerabilities to be detected and remediated prior to release into production, eliminating the cybersecurity risks that they pose. Reduced False Positives and Errors: CloudGuard Serverless Code Scanning incorporates a range of application security testing solutions.

**Disadvantages :** Because a vulnerability scanning tool also misses vulnerabilities, you have no guarantee that your systems are not vulnerable.

**Limitations :** In order to ensure that the most recent vulnerabilities are found, you need to make sure the tool is continually updated.

**Applications :**

* Public and private code repositories.
* Cloud environments.
* Serverless applications.
* Kubernetes.

1. **Encryption**

Encryption is the process of converting plaintext into ciphertext, making it unreadable to anyone without the decryption key.

**Advantages**: Encryption protects data from unauthorized access, even if it is intercepted.

**Disadvantages**: Encryption can add latency and reduce throughput.

**Limitations:** Encryption relies on the security of the encryption keys, so if the keys are compromised, the data will also be compromised.

**Applications:** Encryption is commonly used in cloud environments to protect data both in transit and at rest.

1. **Identity and Access Management (IAM) solutions**

IAM tools are used to authenticate and authorise users in order to restrict access to cloud resources.

**Advantages**: IAM solutions give you a mechanism to implement the least privilege principle and restrict access to cloud resources.

**Disadvantages**: IAM solutions have drawbacks, including the potential to increase throughput while introducing latency and being difficult to set up and maintain.

**Limitations:** IAM solutions rely on the security of the underlying network, so if the underlying network is not secure, the IAM will also be insecure.  
**Applications:** IAM solutions are commonly used in cloud environments to control access to resources and enforce least privilege principles.

1. **Security Information and Event Management (SIEM) tools**

SIEM tools are used to monitor and analyze security-related data from multiple sources in order to identify potential threats.

**Advantages:** SIEM tools provide a way to monitor and analyze security-related data, making it easier to identify potential threats.

**Disadvantages**: SIEM tools can be complex to set up and maintain, and can also introduce latency and reduce throughput.

**Limitations:** SIEM tools rely on the security of the underlying network, so if the underlying network is not secure, the SIEM will also be insecure.

**Applications:** SIEM tools are commonly used in cloud environments to monitor and analyze security-related data from multiple sources.