National Centre of Excellence
for Cybersecurity Technology Development

A JOINT INITIATIVE BY

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

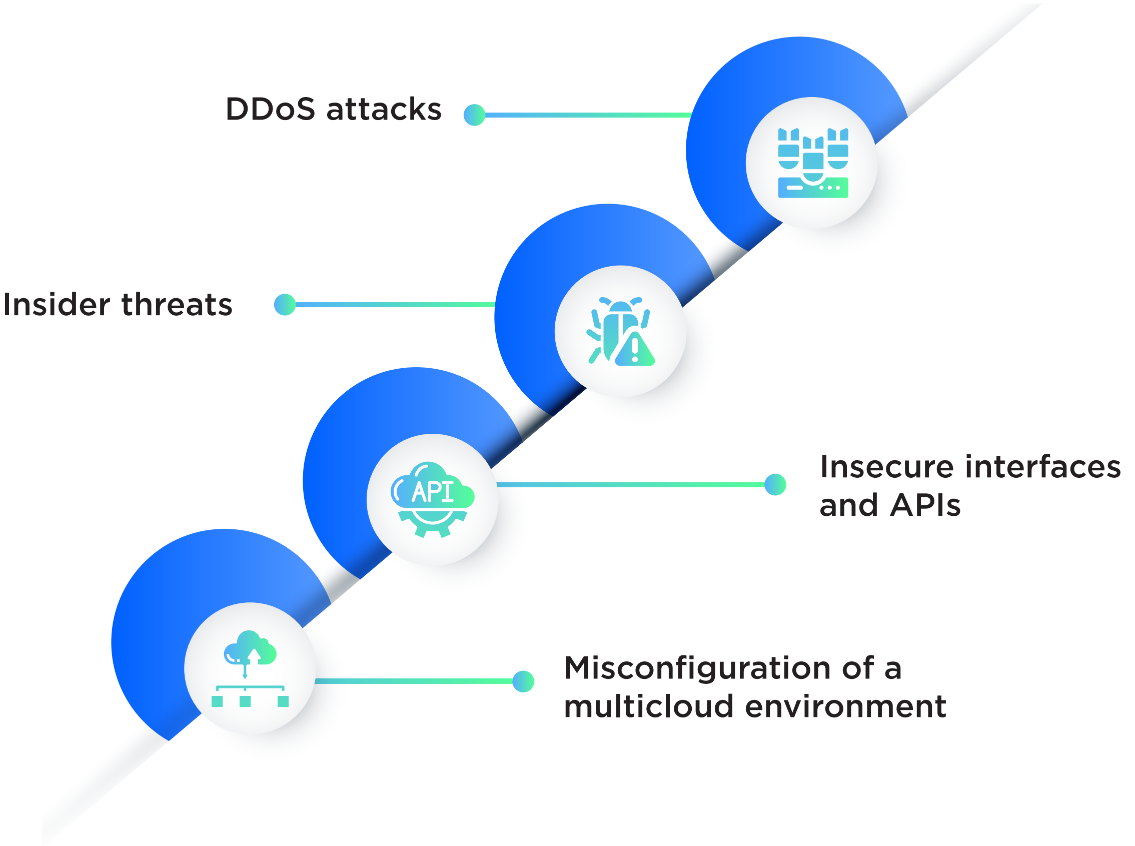
Ministry of Electronics &
Information Technology
Government of India
सत्यमेव जयते

Cloud Security Product Overview

Cloud Security

Cloud security consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data and infrastructure. These security measures are configured to protect data, support regulatory compliance and protect the privacy as well as setting authentication rules for individual users and devices.

Challenges in Cloud Security:



DDoS attacks

Insider threats

Insecure interfaces and APIs

Misconfiguration of a multicloud environment

Organizations are dealing with solutions in the following categories:

01 Encryption solution

02 Network traffic monitoring

03 Authentication along with encrypted transmission

04 Real time visibility

05 API security solution

06 Zero trust security

07 Cloud Access Security Broker (CASB)

08 Granular segmentation to compartmentalize workloads

Zscaler

Cloud based network security
platform and security as a stack

Solution

1. Zscaler Internet Access (ZIA): Secure Internet and web gateway

Methodology

1. Cloud DLP:

- Has predefined dictionaries and preconfigured engines which can be customized.
- Exact Data Match (EDM): Identifies exact records without moving any data to the cloud.
- Sends identified and blocked data over secure ICAP to existing DLP solutions for remediation.
- Streams real-time log events to an external SIEM for further insights.
- Specifies geolocations where logs are written to disk.
- Targets specific users, groups, locations, destinations, and content types with multicriteria policies.
- Provides customized reports and notifications for visibility into DLP violations.

2. Cloud Sandbox

- Provides APT protection — for both inbound and outbound traffic.
- Inspects all traffic, including SSL.
- Optimizes security policies for protection and user experience.
- Enforces policies from a single console.
- Provides inline protection to block threats.

Methodology

3. Cloud Firewall

- Dynamic inspection of HTTP/HTTPS traffic traversing non-standard ports.
- Cloud IPS-
  (1) Transparent updates with the latest signature coverage
  (2) Full SSL inspection.
- Delivers on IPS threat protection and coverage.
- Enables granular firewall policies based on user, location, and application.
- Delivers near-real–time visibility.

4. Bandwidth Control

- Leverage window shaping and bandwidth throttling.
- Break out traffic locally for faster Internet access.
- Reduce MPLS backhaul costs by offloading Internet traffic.
- Enables granular firewall policies.

Deployment

For offices, simply set up a router tunnel (GRE or IPsec) to the closest Zscaler data center. For mobile employees, traffic can be forwarded via lightweight Zscaler App or PAC file.

Zscaler

Cloud based network security
platform and security as a stack

Solution

2. Zscaler Private Access (ZPA): Securing access to the private applications

Methodology

Policies are defined in ZPA Admin Portal and hosted within the Zscaler cloud; Zscaler app is installed; Zscaler app extends a secure micro-tunnel to the Zscaler cloud using App Connector, which is deployed as a VM. The App Connector establishes an outbound connection to the cloud. Within the Zscaler cloud, a Zscaler Enforcement Node is present which approves access and stitches together the user-to-application connection.

1. ZPA for Azure

- Direct-to-cloud access.
- Policy based access.
- Dynamic, application specific TLS-based end to end encryption.

2. ZPA for AWS

- Direct-to-cloud access.
- Policy based access.
- Dynamic, application specific TLS-based end to end encryption.

Deployment

Deployed via an agent.

Hytrust

Security, compliance and control software for virtualization of information technology infrastructure

Solution

1. **Cloud Control:**
Solution offering security and compliance and control for virtual infrastructure

Methodology

Cloud Control

- Offers an End-to-end virtualization security platform to manage access, standardize and control configuration, and protect a virtual infrastructure within a customer's environment.
- Polices are integrated into DevOps style CI/CD environments using “security as code.”
- Functions are automated and integrated using open APIs.
- Two-factor authentication and IAM Integration.

Deployment

It is installed as a virtual appliance.

Hytrust

Security, compliance and control software for virtualization of information technology infrastructure

Solution

2. Data Control:
Strong encryption for virtual machines

Methodology

Data Control

- Encrypts the data on a granular, per VM level.
- Uses powerful encryption engine.
- Protect encrypted workloads against unauthorized access with clone protection.
- Encrypt boot (OS), swap and data Partitions.
- Dynamic partition resizing for Windows VMs.
- AES-NI hardware acceleration in Intel and AMD chipsets helps ensure transparent operation.
- Single encryption key for deduplication support.
- Granular security for Windows and Linux VMs.
- Supports 3rd party hardware Security Modules (HSM) for increased key security.
- Support for encrypting Windows GPT boot drives, including those drives that use UEFI Secure Boot.

Deployment

REST-based API integration for DevOps.

Hytrust

Security, compliance and control software for virtualization of information technology infrastructure

Solution

3. **Key Control:**
Key management system

Methodology

Key Control

- Manage encryption keys for virtual and physical Linux and Windows machines.
- Enables the use of Virtual Trusted Platform Module (vTPM) cryptoprocessors in the VMs.
- High Availability (HA) support with Active-Active cluster (up to 8 KMS servers per cluster).
- Supports the use of TLS 1.2 between all registered clients.
- VMware Certified Key Manager Server (KMS).
- Uses FIPS 140-2 compliant encryption.

Deployment

KeyControl is a VMware certified, scalable, and feature rich KMIP server to simplify key management for encrypted workloads.

Hytrust

Security, compliance and control software for virtualization of information technology infrastructure

Solution

4. Cloud Advisor: Define policies to discover valuable data

Methodology

Cloud Advisor

- Scans a VMs for sensitive data through a content-based policy with defined triggers, either custom or recommended out-of-the box.
- When sensitive data is found, Policy applies the ‘sensitive’ or otherwise pre-defined tag to the VM(s)
- CloudAdvisor deploys and registers the DataControl Policy Agent.
- DataControl initiates encryption of the VM(s) containing sensitive data.

Deployment

Integrated with Microsoft Active Directory to identify user activity related to files stored within a VM.

Hytrust

Security, compliance and control software for virtualization of information technology infrastructure

Solution

5. **Boundary Control:** Policy-based control for virtual workloads

Methodology

Boundary Control

- Provides administrators the ability to comply with national and regional data sovereignty regulations by preventing sensitive applications and data from leaving the datacenter.
- Rooted in Intel Trusted Execution Technology (Intel TXT): Intel TXT provides processor-level attestation of the hardware, BIOS, and hypervisor, allowing sensitive workloads to run on a trusted platform.
- Virtual Server Decryption by Trust and Location.

Deployment

Software and Hardware to enforce geo-fencing to regulatory mandates.

Cipher Cloud

Deep visibility, Adaptive controls and data protection for cloud-mobile environment

Solution

CASB+ Platform:
A gateway that encrypts data in real-time before sending the data into a cloud environment

Methodology

CASB+ Platform

- Verifies the user – Control Access at the door with SSO and MFA integration with IDaaS solutions.
- Cloud apps can be accessed with CipherCloud's Secure Cloud Workspace – Frictionless user interface with secure connectivity to SaaS and private cloud applications.
- Enables contextual access based on managed and unmanaged devices, and geolocation.
- Performs continuous assessment of the security landscape with Adaptive Access Controls.
- Continuously monitors user activity with UEBA (User Entity Behavioral Analytics) for risk.
- Re-evaluates and adapts user access to data and applications using DLP.
- Confirms or terminates the connection based on a user's risk level using step-up authentication.
- Uses data rights management to protect data shared outside of the control.

Deployment

Integrable with custom developed cloud applications without any complex SDK or application modification.

CASB+ is offered in two modes – API-based or Proxy-based: forward and reverse (CipherCloud Mobile Connect).

Spherical Defence

API Security solution using deep unsupervised learning

Solution

Spherical Defence Express:
Protecting the APIs, SaaS and Mobile applications using unsupervised deep learning

Methodology

1. Listen:

- Deploy Spherical instance; Listen for API traffic; Wait for sufficient data to train the first security model.

2. Train:

- The system moves into training mode; Results in a trained security model; spherical instance will continue training more models to account for natural changes in the API traffic.

3. Secure:

- After the security model has been trained; every subsequent API request that is received by the system is given a classification (either benign or anomalous), and a score. All future inbound events are analyzed, and the results returned over HTTP.

Deployment

Integrable on private cloud via docker image and on premise.

Spherical Defence can be installed directly onto the AWS infrastructure using CloudFormation, or alternatively as an Amazon Machine Image.

Illumio

Regulatory compliance, secure
migration of applications to the cloud

Solution

Adaptive Security Platform:
Platform to create granular segmentation to compartmentalize workloads and applications

Methodology

Spherical Defence Express

- The Virtual enforcement Node (VEN) is a lightweight agent which collects and transmits information about the workload's operating system, interfaces, processes, and flows to the Policy Compute Engine (PCE).
- The PCE is the brain that collects all the telemetry information from the VEN, visualizes it via real-time application dependency maps, and then calculates and recommends the optimal firewall rules based on the information about the environment, workloads, and processes.
- The VEN receives applicable firewall rules from the PCE and programs the host's native Layer 3/Layer 4 stateful firewalls. VENs program supported operating systems and containers, as well as ACLs for switches, load balancers, and security groups for clouds (public, private, hybrid).

Deployment

The PCE can be deployed via Illumio's SaaS platform, on premises, and in a virtual private cloud. The VEN is installed in the guest OS of the host.

Obsidian Security

Threat detection, breach remediation, and security hardening for SaaS

Solution

Obsidian Cloud Detection and Response:
Threat detection, breach remediation, and security hardening for SaaS

Methodology

Obsidian Security

- Services need to be onboarded to Obsidian by using API connection.
- Collects, normalizes the data from the cloud applications and enriches with threat intelligence.
- Constructs the Obsidian Identity Graph, an intuitive data model to understand users, privileges, and activity.
- Generates alerts around breaches and insider threats informed by machine learning analytics and rules.
- Learns from the user behavior at the individual, group and organization level.
- Recommendations are made to harden the security of cloud applications.

Deployment

The Obsidian platform is delivered as SaaS through API integrations.

About DSCI's
National Centre of Excellence

DSCI's National Centre of Excellence (National CoE) is a Joint Venture between Data Security of India (DSCI) and the Ministry of Electronics and Information Technology (MeitY) with the objective of providing impetus to the startup ecosystem in India. DSCI has set up a facility, which houses technology research lab, experience zone for demonstration of national cyber capability, experimental SOC, co-creation spaces, training facility for niche capability building, and an incubation center.

This is a content series for National Centre of Excellence to dissect the emerging security technology products to reveal usecases, technology stack and deployment strategies. This effort is to create awareness and understanding of technology and not to promote any particular product or company.

@nationalcoe

@CoeNational

company/nationalcoe

www.dsci.in/content/national-centre-excellence-cyber-security-technology-development

ncoe@dsci.in