DuploCloud

WHITEPAPER

Accelerating SOC 2 Compliance by Integrating Security into Cloud Operations

Contents

Introduction

SOC 2 is a popular standard that is used across a broad set of industries. If you are a service provider or a service organization which stores, processes, or transmits any kind of information, businesses are increasingly looking to ensure you have the controls in place before trusting you with their data. This necessitates 3rd party security reports such as a SOC 2, recent Pen Test report and/or collaboration on a detailed InfoSec questionnaire. In order to stay competitive, it's increasingly common for technology and SaaS companies to have these documents readily available to customers upon request.

For your SOC 2 certification, you will need to consider controls for:

1. **People, process and documented policies**
2. **Implementation and subsequent verification of infrastructure security**
3. **Any additional controls that concern current and future customers (commonly detailed in InfoSec questionnaires)**

Thankfully, it has become significantly easier and faster, particularly for small organizations to achieve their SOC 2 compliance. Technology advancements have impacted cloud providers, small businesses and auditors to streamline the process of implementing and validating each control. In particular, a handful compliance automation software vendors have emerged that help with people and process policies, and create a view for both businesses and auditors, to align on control gaps as you work towards SOC 2. With DuploCloud, you can achieve out-of-the-box compliance for both 2 and 3.
The next section of this white paper describes DuploCloud's approach for a SOC 2 Implementation.
The final section, is a detailed controls matrix mapping each SOC 2 requirement to the DuploCloud Implementation.

It is a common misconception that if the cloud provider is SOC 2 compliant, the organization hosting the application on the provider is also certified. The cloud is a shared security model, requiring consumers to be responsible to configure the services provided by the cloud vendor to meet security requirements. A simple example is a web application that is exposed to the internet with all ports open. The blame squarely lies with the business, not the cloud provider.

DuploCloud Approach

DuploCloud is a DevSecOps software platform that builds and operates a fully compliant infrastructure on your behalf based on SOC 2 and other desired security controls and compliance standard.

DuploCloud automates and integrates DevOps configurations, security tools, and cloud APIs to build and operate a fully compliant and secure infrastructure. Unlike other security or DevOps tools that operators integrate into their infrastructure to perform a specialized siloed function, DuploCloud is fundamentally a labor optimization solution reducing implementation hours from 6 months to one week.

To implement any infrastructure control, the first preference is a native solution by the cloud provider. This constitutes about 90% of the controls which are implemented by orchestrating those feature sets in AWS, Azure, or GCP via APIs. Next, standard community software is considered for any remaining controls. For example, WAZUH as SIEM (security, incident and event managements), ClamAV for antivirus, and Suricata for NIDS (network intrusion detection system). Finally, for remaining controls or based on customer preference for a certain tool, the framework integrates third-party ISV tools. This extensibility is available useradded plugins as well. For example, currently DuploCloud is integrated with Sentry for alerting, Jira for incident management, Sumo Logic for log collection, and SignalFx for metrics.

At an architecture level, DuploCloud operates with the following five declarative specifications:

1. **Product Architecture**
2. **Availability requirements**
3. **Scale needs**
4. **Compliance Standard**
5. **Cost considerations**

Internally, the software is a rules-based engine that combines these requirements with cloud subject matter expertise – IAM, AD policies, security group rules, availability zones, regions, etc. – compliance guidelines – such as separation of production and stage into different networks – and runs all this through a state machine to produce the desired output. The state machine is constantly active post-configuration and reconciles or alerts on any drift. Updates go through the same process.

Self-Hosted

DuploCloud is single tenant software that installs in either your cloud account or in our cloud account dedicated to you. User's interface with software via the browser UI and/or API calls. All data and configuration stays within your cloud account. All configurations that have been created and applied by the software are transparently available to be reviewed and edited in your cloud account. All configuration information and data stays with you and is controlled by you.

Policy Model

DuploCloud exposes a declarative policy model which forms the basis of the implementation. Following is a brief overview. Detailed product documentation is available here: AWS User Guide, Azure User Guide.

- **Infrastructure**. An infrastructure maps 1:1 with a VPC/VNET and can be in any region. Each infrastructure has a set of subnets spread across multiple availability zones. In AWS there is a NAT gateway for private subnets.
- **Tenant or Project.** Tenant is the most fundamental construct of the policy model. It represents an application's entire lifecycle. It is:
  - A security boundary i.e., all resources within a tenant have access to each other, but any external access is blocked unless explicitly exposed via an LB, IAM/AD Policy, or SG.
  - A container of resources with each resource implicitly tagged with the tenant name and other labels associated with the tenant. Deleting a tenant deletes all the resources underneath. In Azure, a tenant is a resource group.
  - An access control boundary i.e., each tenant can be accessed by N number of users and each user can access M tenants. The single sign on access given for a user to a tenant is automatically propagated to provide just-in-time access to the AWS and Azure resources via the console by the software.
  - Carries all the logs, metrics, and alerts of the application in a single dashboard.
  - Links to the application's code repository for CI/CD, providing a runtime build as a microservice construct such that each tenant can run its own builds in 6 © 2022 DuploCloud, Inc. resources in that tenant without worrying about setting up a build system like Jenkins, etc.
  - Part of 1 and only 1 infrastructure. An infrastructure can have multiple tenants.
- **Plan**. This is a logical construct and a container of tenants. It basically has governance policies for the tenants under it. For example, resource usage quota, allowed AMIs, allowed certificates, labels, etc. Each plan can be linked to one and only one infrastructure.
- **User**. This is an individual with a user ID. Each user could have access to one or more tenants/projects.
- **Host**. This is an EC2 instance or VM. This is where your application will run.
- **Service**. Service is where your application code is packaged as a single docker image and running as a set of one or more containers. It is specified as - image-name; replicas; env-variables; vol-mappings, if any. DuploCloud also allows running applications that are not packaged as Docker images.
- **LB**. A Service can be exposed outside of the tenant\project via an LB and DNS name. LB is defined as - Service name + container-port + External port + Internal-orinternet facing. Optionally, a wild card certificate can be chosen for SSL termination. You can choose to make it internal which will expose it only within your VPC/VNET to other applications.
- **DNS Name.** By default, when a Service is exposed via an LB, DuploCloud will create a friendly DNS Name. A user can choose to edit this name. The domain name must have been configured in the system by the admin.

- **Docker Host or Fleet Host**. If a host is marked as part of the fleet, then DuploCloud will use it to deploy containers. If the user needs a host for development purposes such as a test machine, then it would be marked as not part of the pool or fleet.

Agent Modules

For many of the compliance controls, several agent-based software packages are installed in each VM that is in scope. A few examples are the Wazuh agent to fetch all the logs, ClamAV virus scanner, AWS Inspector that provides vulnerability scanning, Azure OMS and CloudWatch agents for host metrics. While these agents are installed by default, DuploCloud provides a framework where the user can specify an arbitrary list of agents in the following format and DuploCloud will install these automatically in any launched VM. If any of these agents crash, then DuploCloud will send an alert. One good use case is to monitor the health of the ClamAV agent.

In the DuploCloud UI this configuration is under Security → Agents Tab

```
[
        {
                "AgentName":"AwsAgent",
                "AgentWindowsPackagePath":"https://inspector-
agent.amazonaws.com/windows/installer/latest/AWSAgentInstall.exe",
                "AgentLinuxPackagePath":"https://inspector-
agent.amazonaws.com/linux/latest/install",
                "LinuxAgentInstallStatusCmd":"sudo service --status-all |
grep -wc 'awsagent'",
                "WindowsAgentServiceName":"awsagent",
                "LinuxAgentServiceName":"awsagent",
                "LinuxInstallCmd":"sudo bash install"
        },
        {
                "AgentName":"ClamAV_v0",
                "AgentWindowsPackagePath":"",
       "LinuxAgentInstallStatusCmd":"sudo service clamav-freshclam status |
grep -wc 'running'",
                "AgentLinuxPackagePath":"https://www.google.com",
                "WindowsAgentServiceName":"",
                "LinuxAgentServiceName":"clamav-freshclam",
                "LinuxInstallCmd":"OS_FAMILY=$(cat /etc/os-release | grep
PRETTY_NAME); if [[ $OS_FAMILY == *'Ubuntu'* ]]; then sudo apt-get update;
sudo apt-get install -y clamav; else sudo amazon-linux-extras install -y
epel; sudo yum install clamav clamd -y; sudo service clamav-freshclam
start; fi",
                "LinuxAgentUninstallStatusCmd":"OS_FAMILY=$(cat /etc/os-
release | grep PRETTY_NAME); if [[ $OS_FAMILY == *'Ubuntu'* ]]; then sudo
apt-get autoremove -y --purge clamav; else sudo yum remove -y clamav*; fi"
        },
        {
                "AgentName": "clamav_scanner_v2",
                "AgentWindowsPackagePath": "",
                "AgentLinuxPackagePath": "https://www.google.com",
                "WindowsAgentServiceName": "",
                "LinuxAgentServiceName": "clamav-freshclam",
                "LinuxInstallCmd": "sudo unlink
/etc/cron.hourly/clamscan_*; sudo wget -O installclamavcron.sh
https://raw.githubusercontent.com/duplocloud/compliance/master/installclama
vcron.sh; sudo chmod 0755 installclamavcron.sh; sudo
./installclamavcron.sh",
                "LinuxAgentInstallStatusCmd": "ls -la /etc/cron.hourly |
grep -wc 'clamscan_v1_hourly'",
                "LinuxAgentUninstallStatusCmd": "unlink
/etc/cron.hourly/clamscan_v1_hourly"
        }
]
```

Prerequisite Reading

View the following two videos on DuploCloud's website to become familiar with the concepts of DuploCloud before reading through the control implementation details.

Explainer Video: https://vimeo.com/407475394
Product Demo: https://vimeo.com/577816574
Product Documentation and concepts: https://docs.duplocloud.com/docs/

More information is available @ www.duplocloud.com

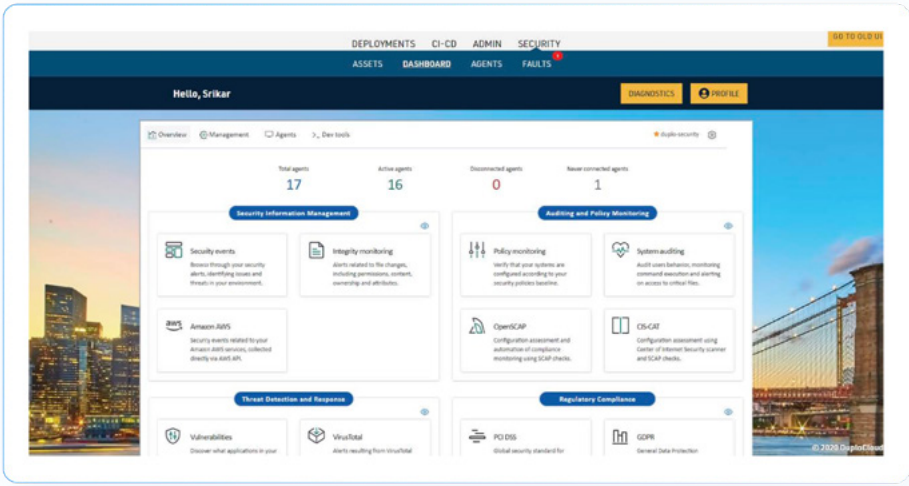
Security Information and Event Management

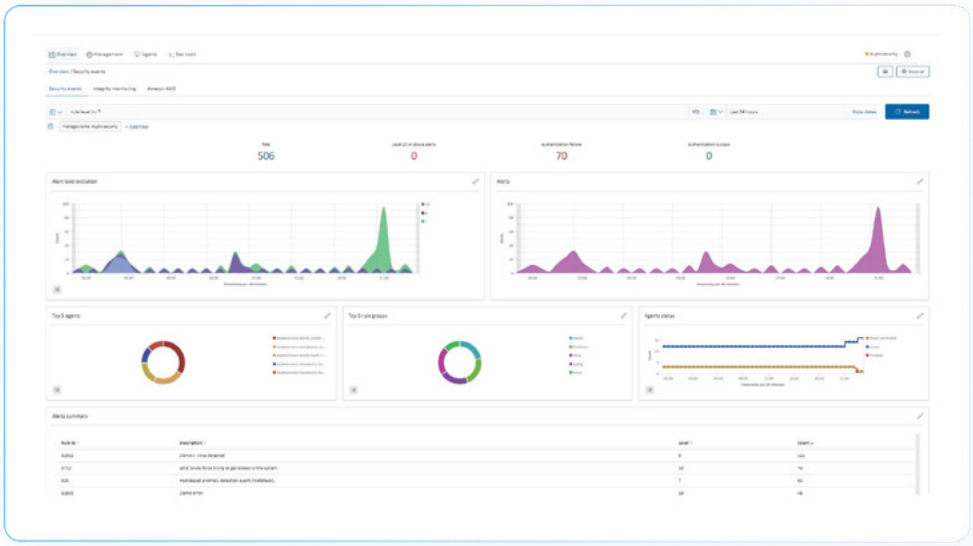
Every infrastructure has a centralized system to aggregate and process all events. The primary functions of the system are:

1. **Data Repository**
2. **Event Processing Rules**
3. **Dashboard**
4. **Events and Alerting**

Distributed agents of this platform are deployed at various endpoints (VMs in Cloud) where they collect events data from various logs like syslogs, virus scan results, NIDS alerts, File Integrity events, etc. Data is sent to a centralized server and undergoes a set of rules to produce events and alerts that are stored in typically Elasticsearch where dashboards can then be generated. Data can also be ingested from sources like CloudTrail, AWS Trusted Advisor, Azure Security Center and other non-VM based sources.

The strength of an SIEM is fundamentally judged by two factors: Rules set and Data parser. Together these determine the amount of coverage. Wazuh is a fantastic SIEM with the most elaborate coverage. Any required security functionality has its ruleset in Wazuh, be it FIM, CVE, Virus Scanning or CloudTrail. At the same time, the Wazuh platform is extensible, open source and has over 1.5K GitHub stars and 369 GitHub forks. Subsequent sections describe the location of various core modules of our SOC 2 implementation in the Wazuh dashboard.





Provisioning Features (DevOps)

DuploCloud platform is both a provisioning as well as monitoring system. By virtue of the provisioning capabilities the platform can account for all the required compliance controls as against other security and GRC tools (like Prisma cloud, alert logic, laceworks) that have a role purely post provisioning and hence account for only a small minority of security controls. While there are hundreds of resource provisioning features as described in https://docs.duplocloud.com/docs/, they can be broadly categorized as follows:

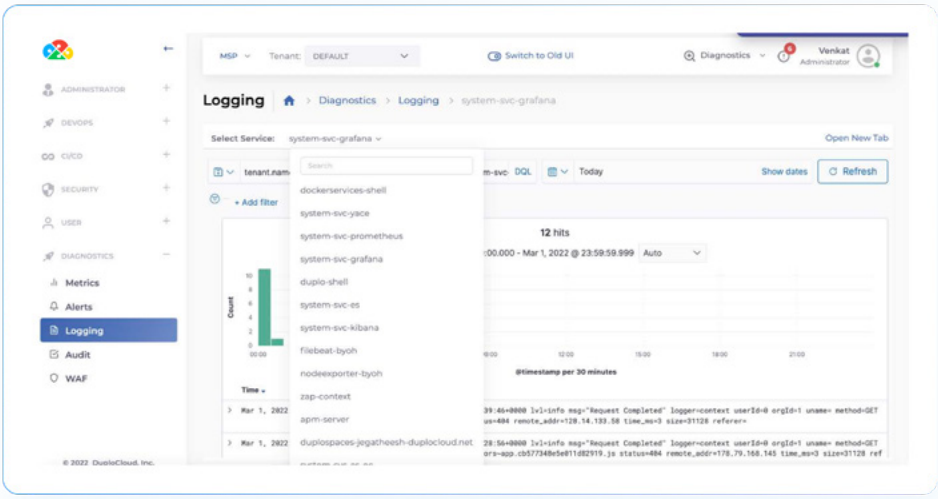
- Network Provisioning and Landing zones that includes VPC/VNET/VPN
- Access control roles and policies using cloud provider IAM
- Encryption at rest using cloud provider key management systems like KMS, Azure Key Vault etc.
- Transport Encryption (transit) using certificates that involves configuring load balancers, gateways, and certificate managers.
- Secrets management using secret stores like AWS secret store, Azure Key Vault, Kubernetes secrets
- Provisioning scores of cloud native services like s3, Dynamo, Azure storage, Kafka, Elastic Search etc. This includes tying together various access policies, availability considerations, scale, and of course various compliance configuration. As an example, while S3 setting up the system manages SSE, public access block, versioning (when needed), IAM access control among other things. The exhaustive list of these features is described on the user guide https://docs.duplocloud.com/docs/
- Application provisioning tool orchestration. For example, for containerized workloads the system manages EKS/AKS/GKE, ECS/Azure webapps, Spark, EMR, Data pipelines for big data, Lambda, Azure Functions and GCP for serverless workloads and finally Sage Maker and Kubeflow for AI/ML

Monitoring Features (SecOps)

Post provisioning, DuploCloud orchestrates third party open source and cloud provider monitoring solutions to validate the security and compliance posture as well as detect drift in desired state and alert. Using third party tools thus provides an independent attestation of the earlier described provisioning system. Following are these set of features

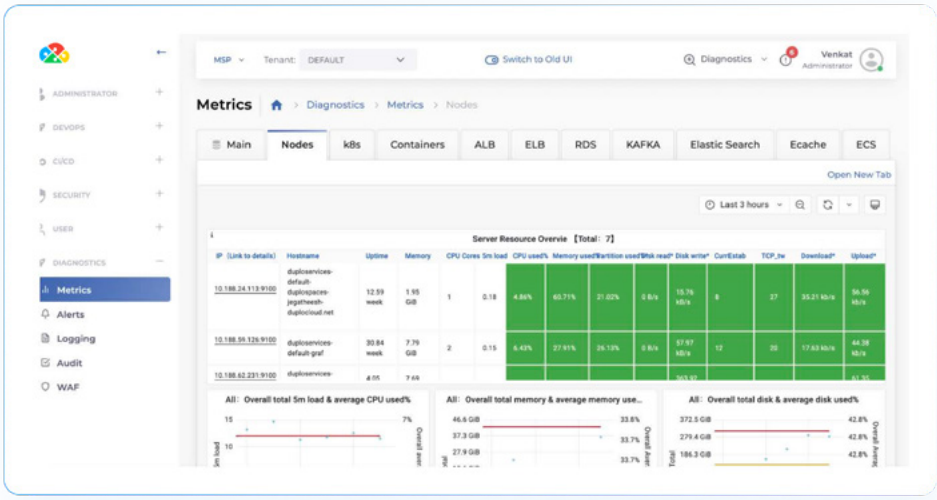
Central Logging via Elastic Search

ELK stack is deployed in a separate tenant and file beat containers deployed in individual tenants. The setup automatically inserts various metadata required to segregate the logs into separate tenants, services, and hosts.



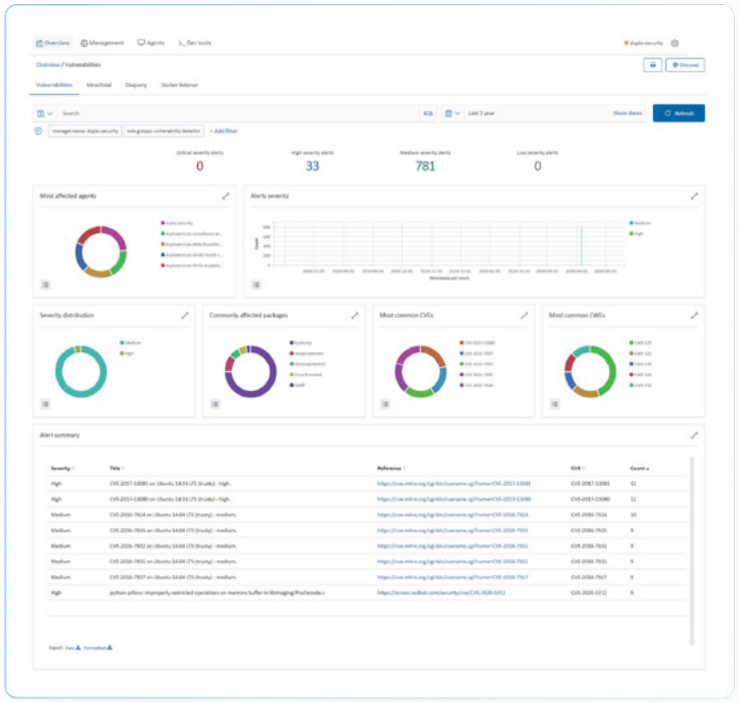
Metrics via Prometheus, Grafana and Cloud Watch

Prometheus and Grafana containers are deployed in a separate tenant. Node exporter, **CADvisor** and **CloudWatch** agents are deployed in individual tenants. Metrics are segregated with tenants, services and out-of-box dashboards are made available.



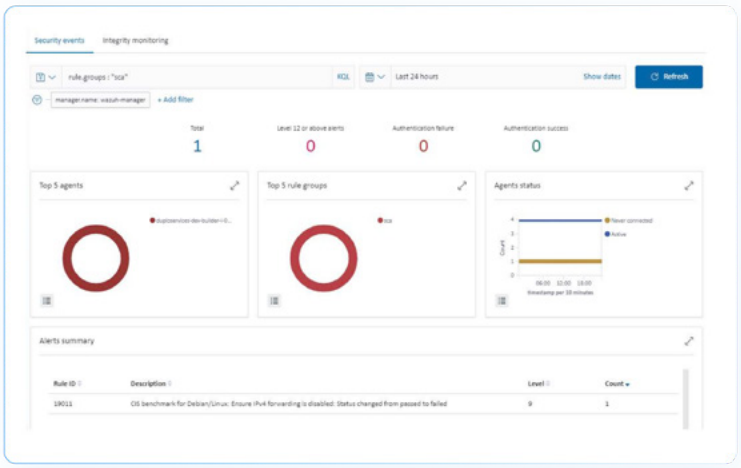
Vulnerability Detection

Agents collect the list of all installed applications and send it to the Wazuh master which compares with global vulnerability database using public OVAL CVE repositories. To check the vulnerabilities, go to “Security dashboard Vulnerabilities”. For more information on the implementation, refer to the Wazuh Vulnerability Detection Guide.



CIS Benchmarks

Wazuh provides the Security Configuration Assessment (SCA) module which offers the user the best possible experience when performing scans on hardening and configuration policies. To check the SCA report, go to “Security dashboard → Security Events” and search for rule.groups: “sca”. For more information, refer to the Wazuh SCA.

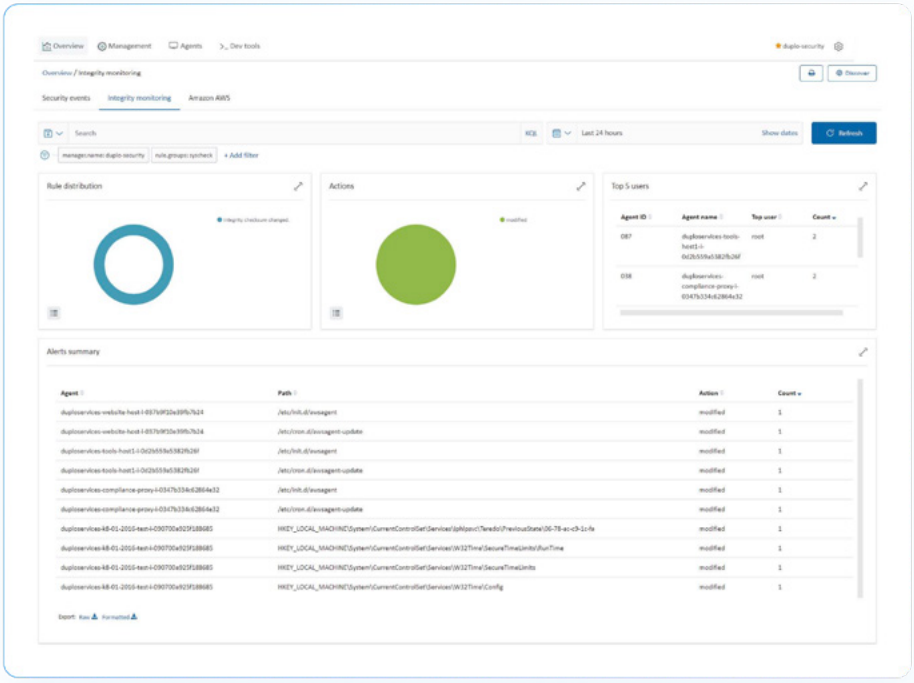


Cloud Vulnerabilities & Intrusion Detection

DuploCloud integrates and orchestrates AWS Inspector, CloudTrail, Trusted Advisor, VPC flow logs and GuardDuty. To view the alerts, go to “SIEM Dashboard → Amazon AWS”. Following is an example of an alert for a break-in attempt into AWS Console:

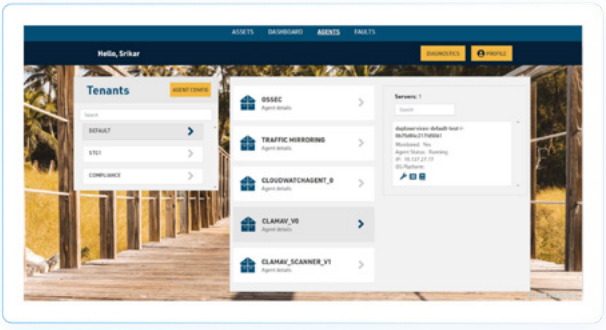
File Integrity Monitoring

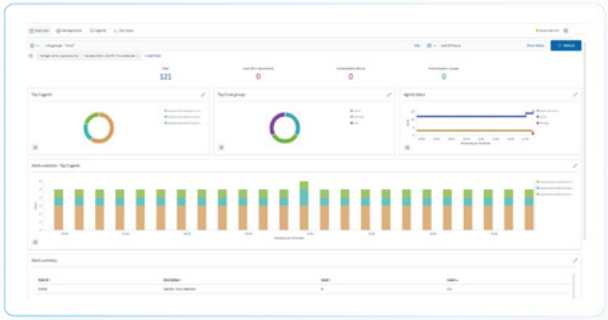
Agents on the hosts will monitor the key files for any changes, verifying the checksum and attributes of the monitored files. The System Check will happen every 12 hours. To check the file integrity monitoring, go to “SIEM Dashboard → Integrity Monitoring”. For more information, refer to the Wazuh Vulnerability Detection Guide.



Virus Scanning

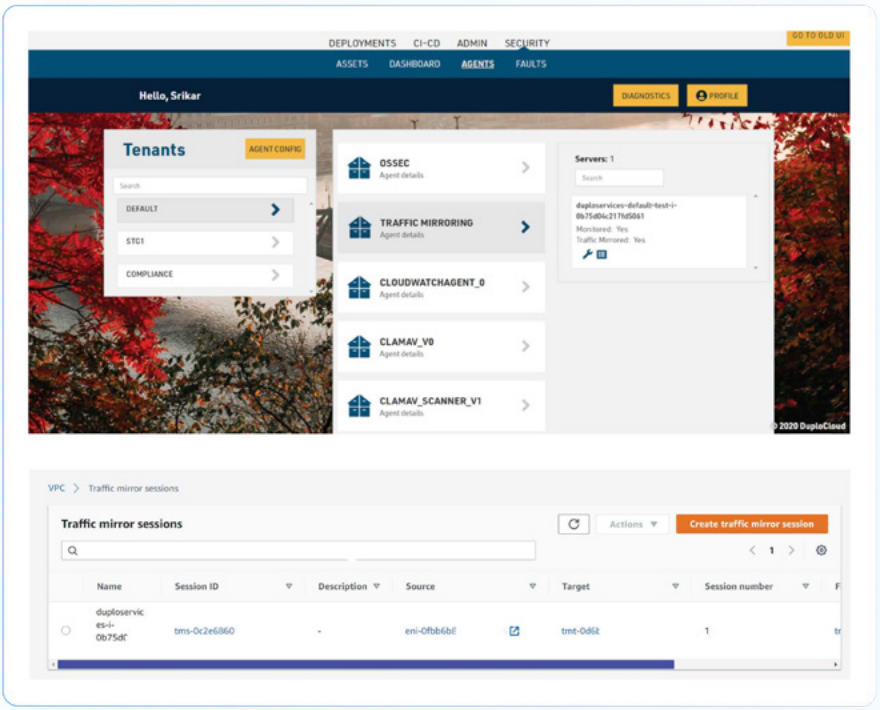
DuploCloud enables ClamAV deployment via agent modules, with alerts collected and categorized in SIEM. Make sure the ClamAV agent module is enabled in DuploCloud. For more information on how to enable this, refer to the config in the “Other Agents” section. DuploCloud will make sure that the ClamAV agent is running and if it fails a fault is raised in the DuploCloud portal. To view the virus alerts, go to “SIEM Dashboard → Security Events → Add a filter (rule.groups: virus)”.

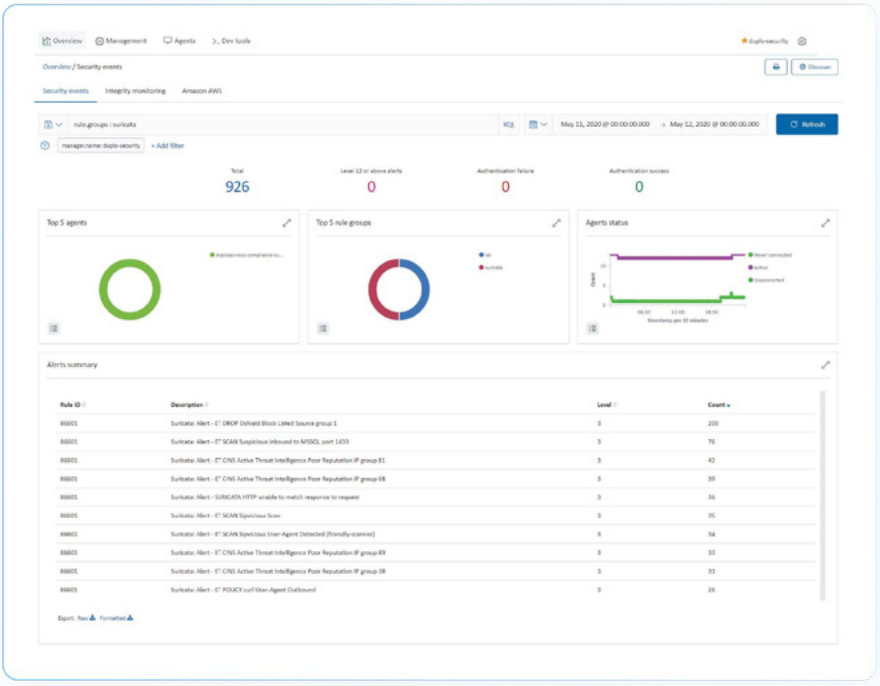




Network Intrusion Detection

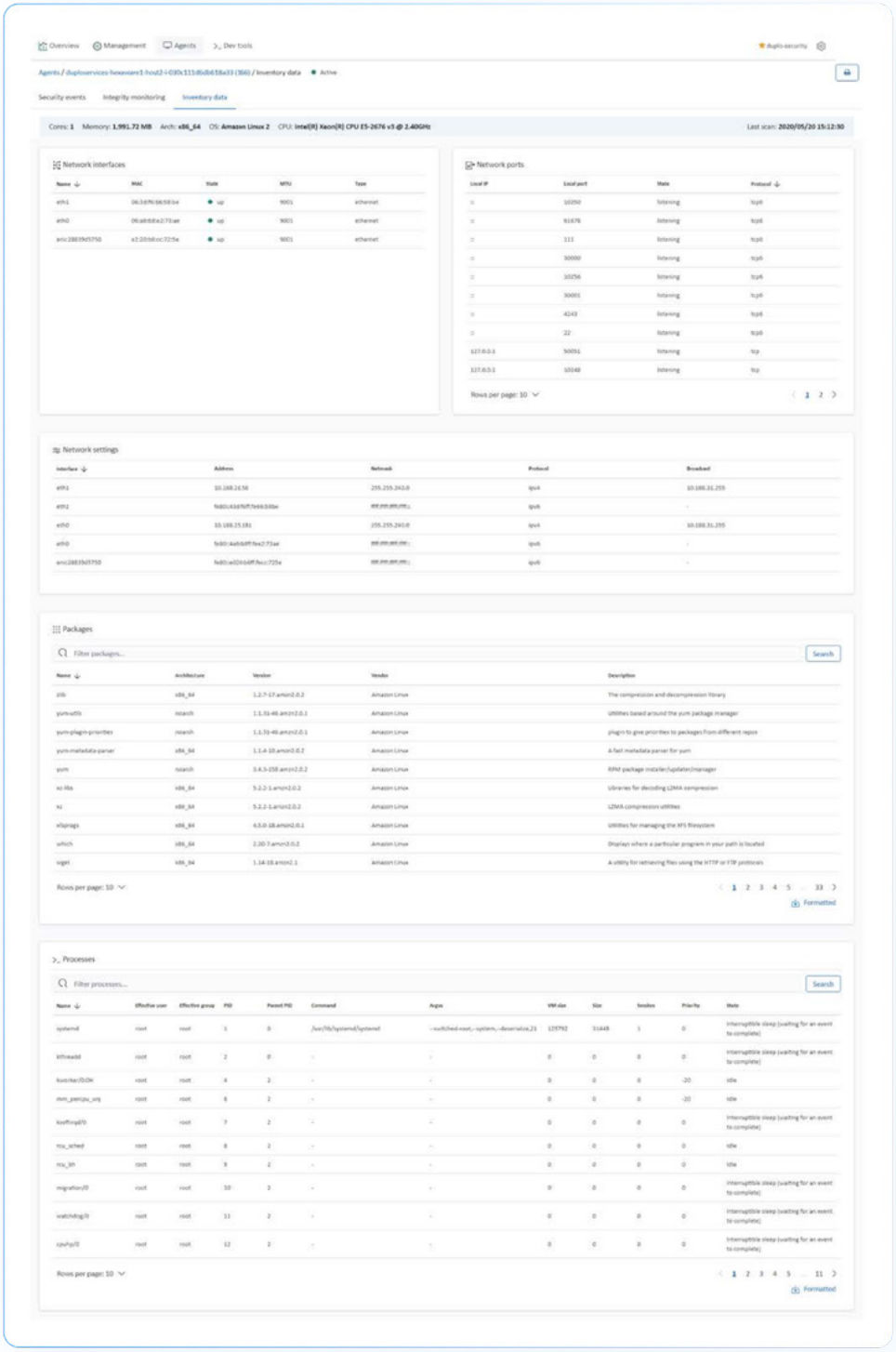
DuploCloud uses Suricata as a NIDS processing engine. The traffic mirroring capability in AWS is employed to not bog down the hosts with additional services. We spawn a host which has Suricata running, and it is the target of mirrored traffic from all hosts. Suricata analyses this traffic and produces results in files that are collected by Wazuh agents, then sent to the SIEM. To check the network vulnerabilities, go to "SIEM Dashboard → Security Events → Add in search (rule.groups: "suricata")". Refer to AWS Traffic mirroring and Suricata.





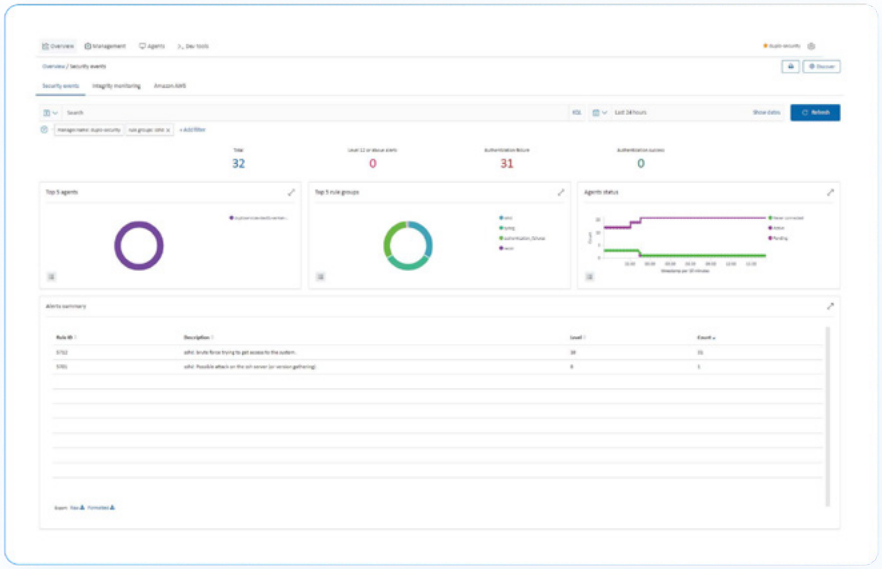
Inventory Management

DuploCloud collects and stores inventory information from the Cloud infrastructure and at an operating system level from each host. It also has an inventory of all the Docker containers currently running in the server. For Cloud inventory, go to “Security → Assets”, for Docker containers, look at “Admin → Metrics” and for OS level inventory (Installed apps, network configuration, open ports, etc.), go to “SIEM Dashboard → Agents → Select agent of your choice → Select inventory data”. For more information refer to System Inventory.



Host Intrusion Detection

Agents installed by DuploCloud will combine anomaly and signature-based technologies to detect intrusions or software misuse. They can also be used to monitor user activities, assess system configuration, and detect vulnerabilities.



Host Anomaly Detection

Anomaly detection refers to the action of finding patterns in the system that do not match the expected behavior. Once malware (e.g., a rootkit) is installed on a system, it modifies the system to hide itself from the user. Although malware uses a variety of techniques to accomplish this, Wazuh uses a broad-spectrum approach to finding anomalous patterns that indicate possible intruders. This includes:

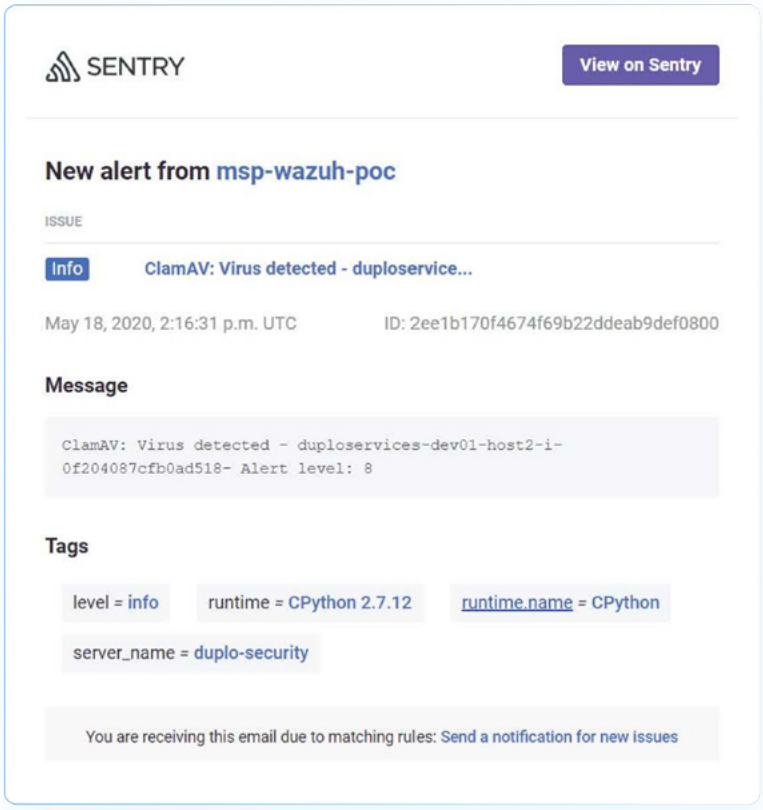
- **File integrity monitoring**
- **Check running process**
- **Check hidden ports**
- **Check unusual files and permissions**
- **Check hidden files using system calls**
- **Scan the /dev directory**
- **Scan network interfaces**
- **Rootkit checks**

For more information refer to [Wazuh Anomaly Detection.]

```
** Alert 1460225922.841535: mail  - ossec,rootcheck
2017 Feb 15 10:00:42 (localhost) 192.168.1.240->rootcheck
Rule: 510 (level 7) -> 'Host-based anomaly detection event (rootcheck).'
Process '495' hidden from /proc. Possible kernel level rootkit.
```

Email Alerting

DuploCloud extends Wazuh with an alerting module to send alerts to Sentry which in turn sends the email alerts. All the alerts above a configured level (default is 7) will be sent as an email to the configured users in Sentry.



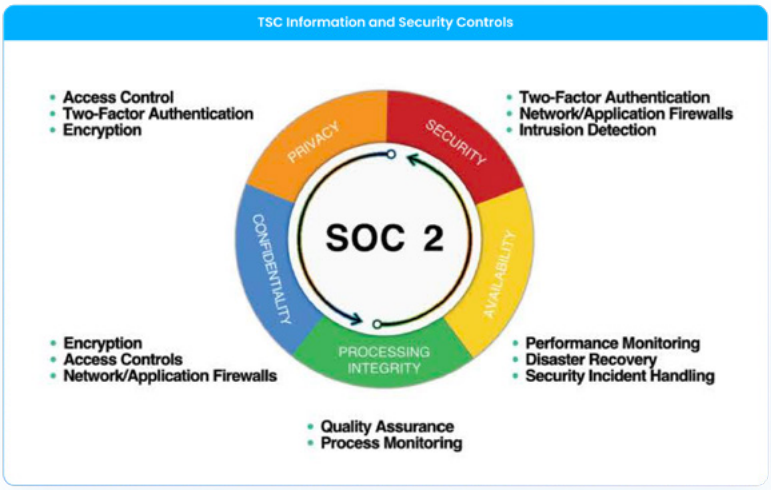
Incident Management

Sentry has integration with Jira. All the events that come to Sentry can be configured to create incidents in Jira. For more information refer to Sentry Jira Integration.

SOC 2 compliance controls

AICPA Trust Services Criteria (TSC)
Service and Organization Controls as a standard was introduced by the Association of Independent Certified Public Accountants (AICPA) and is based on the Trust Services Criteria (TSC). Each TSC is divided into Points of Focus which can be a security control or a combination of security controls or linked to one or some security controls. These controls can be categorized as either technical or process oriented. In either case, documentation and validation is required for all SOC 2 audits.

For a detailed breakdown of the Trust Service Criteria, you can download AICPA trust services criteria PDF here.



The Trust Service Criteria are modeled around the following areas:

- Security (Core in all TSC information and system controls): Control Environment (CC1.x), Communication and Information (CC2.x), Risk Assessment (CC3.x), Monitoring Activities (CC4.x), Control Activities (CC5.x), Logical and Physical Access Controls (CC6.x), System Operations (CC7.x), Change Management (CC8.x), Risk Mitigation (CC9.x)
- Additional criteria for Availability (A1.x)
- Additional criteria for Confidentiality (C1.x)
- Additional criteria for Processing Integrity (PI1.x)
- Additional criteria for Privacy (P1.x)

The security guidelines from various standards have a large overlap. While DuploCloud can automate the provisioning of cloud applications adhering to the more stringent PCI-DSS or HIPAA standards, this document describes the controls implemented by DuploCloud mapping to SOC 2.

Point of focus	Trust Criteria	DuploCloud Implementation
Logical and Physical Access Controls (CC 6.1) The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives		
1	*Identifies and Manages the Inventory of Information Assets—The entity identifies, inventories, classifies, and manages information assets.*	DuploCloud provides a single management portal for all changes related to cloud infrastructure. All infrastructure assets are classified into "Tenants" that provide an application centric abstraction. Further, agents are deployed inside the virtual machines that track down the inventory in terms of application packages.
2	*Restricts Logical Access— Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets.*	DuploCloud tenant model has access controls built in. This allows access to various tenant based on the user roles. This access control mechanism automatically integrates into the VPN client as well i.e., each user has a static IP in the VPN and based on his tenant access his IP is added to the respective tenant's SG. Tenant access policies will automatically apply SG or IAM based policy based on the resource type. DuploCloud by default orchestrates appropriate services like Encryption at rest and transit to protect data integrity.
3	*Identifies and Authenticates Users—Persons, infrastructure and software are identified and authenticated prior to accessing information assets, whether locally or remotely.*	DuploCloud integrates with the client's IDP like Gsuite and O365 for access to the portal. From there a federated logic is done for AWS resource access and this access is Just-in-time. This enables a mechanism where no individual users need to be created or managed at cloud provider level. For access into container and VM shells technologies like Cloud Bash and SSM (AWS) are integrated.
4	*Considers Network Segmentation—Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.*	Infrastructure is split into public and private subnets. Dev, stage, and production are split into different VPCs/VNETs. DuploCloud automation introduces a concept of a tenant which is a logical construct above AWS/Azure and represents an application's entire lifecycle. It is a security boundary implemented by having a unique SG, IAM Role and Instance Profile in AWS/ a Subnet, NSG and Managed Identity in Azure per tenant. By default, no access is allowed into the tenant unless specific ports are exposed via LB. The application is split into multiple tenants with each tenants having all private resources in a private subnet. An example implementation would be all data stores are in one tenant and the frontend UI is in a different tenant.
5	*Manages Points of Access— Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed.*	DuploCloud's scope is at the level of cloud infrastructure resources. All resources are by default placed in an internal network and external access is granted by specific resources only like Load balancers, bastions and selected VMs on public IP (when needed). The DuploCloud management portal as well as Infrastructure-as-code approach (https://duplocloud.com/white-papers/devops/) provides the needed identification, documentation, and management.
6	*Restricts Access to Information Assets—Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access control rules for information assets.*	Infrastructure is split into public and private subnets. Dev, stage, and production are split into different VPCs/VNETs. DuploCloud automation introduces a concept of a tenant which is a logical construct above AWS/Azure and represents an application's entire lifecycle. It is a security boundary implemented by having a unique SG, IAM Role and Instance Profile in AWS or a Subnet, NSG and Managed Identity in Azure per tenant. By default, no access is allowed into the tenant unless specific ports are exposed via LB. The application is split into multiple tenants with each tenants having all private resources in a private subnet. An example implementation would be all data stores are in one tenant and the frontend UI is in a different tenant. Internally, the platform uses cloud resources like IAM, AD, Security groups, certificates, Encryption Keys and other necessary artifacts to implement an application centric abstraction to establish access control rules for information assets.

7	*Manages Identification and Authentication—Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure and software.*	DuploCloud integrates with client's IDP like Gsuite and O365 for access to the portal. From there a federated logic is done for AWS resource access and this access is Just-in-time. This enables a mechanism where no individual users need to be created or managed at cloud provider level. For access into container and VM shells technologies like Cloud Bash and SSM (AWS) are integrated. The DuploCloud management portal as well as Infrastructureas- code approach (https://duplocloud.com/white-papers/devops/) provides the needed identification, documentation, and management.
8	*Manages Credentials for Infrastructure and Software— New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required, or the infrastructure and software are no longer in use.*	All infrastructure changes are centralized via DuploCloud. Access to users is via Single sign on. From there on an individual cloud resource basis access is automatically generated to the cloud portal as a Just-in-time credentials. This is done by called cloud providers federated APIs. No individual user access needs to be maintained in cloud provider. Typical default time space for JIT access is configurable and ranges from 15 mins to a couple of hours.
9	*Uses Encryption to Protect Data—The entity uses encryption to supplement other measures used to protect data-at-rest, when such protections are deemed appropriate based on assessed risk.*	DuploCloud by default orchestrates appropriate services like Encryption at rest and transit to protect data integrity. For data at rest DuploCloud orchestrates KMS keys per tenant to encrypt various AWS resource in that tenant like RDS DBs, S3, Elastic Search, REDIS etc. For data in transit DuploCloud fetches the certificates from cert manager and all the requests can be made through TLS.
10	*Protects Encryption Keys— Processes are in place to protect encryption keys during generation, storage, use, and destruction.*	DuploCloud orchestrates AWS KMS/Azure Key Vault keys per tenant to encrypt various AWS/Azure resource in that tenant like DBs, S3, Elastic Search, REDIS etc. Access to the keys is granted only to the instance profile w/o any user accounts or keys. By default, DuploCloud creates a common key per deployment, but allows ability to have one key per tenant.

Logical and Physical Access Controls (CC 6.2)

Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

1	*Controls Access Credentials to Protected Assets—Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian.*	DuploCloud integrates with the client's IDP like Gsuite and O365 for access to the portal. Within the portal the user access is limited by tenants. Administrators of the system manage access for users at a tenant level which is an application centric abstraction rather than having to do it at the lower layer in the cloud provider that would have required access to be managed across hundreds of resources. All access management operations are tracked and audited in an Elastic Search instance.
2	*Removes Access to Protected Assets When Appropriate— Processes are in place to remove credential access when an individual no longer requires such access.*	Access to users is via Single sign on. From there on an individual cloud resource basis access is automatically generated to the cloud portal as a Just-in-time credentials. This is done by called cloud providers federated APIs. No individual user access needs to be maintained in cloud provider. Typical default time space for JIT access is configurable and ranges from 15 mins to a couple of hours.
3	*Reviews Appropriateness of Access Credentials—The appropriateness of access credentials is reviewed on a periodic basis for unnecessary and inappropriate individuals with credentials.*	Having a centralized management portal along with an application centric abstraction (Tenant) to which access is tied allows an organization to easily go through the review of access on a periodic basis. This would have been a very laborious effort if one had to do it at an individual cloud resource level that would have spanned into hundreds and thousands of lines of code.

Logical and Physical Access Controls (CC 6.3)

The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.

1	*Creates or Modifies Access to Protected Information Assets— Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.*	DuploCloud integrates with client's IDP like Gsuite and O365 for access to the portal.
2	*Removes Access to Protected Information Assets—Processes are in place to remove access to protected information assets when an individual no longer requires access.*	DuploCloud integrates with client's IDP like Gsuite and O365 for access to the portal. The moment the email is disabled all access is revoked. Even if the user has a private key to a VM even then he cannot connect because VPN will be deprovisioned.
3	*Uses Role-Based Access Controls—Role-based access control is utilized to support segregation of incompatible functions.*	DuploCloud integrates with client's IDP like Gsuite and O365 for access to the portal. Within the portal the user access is limited by tenants which provides the segregation. Administrators of the system manage access for users at a tenant level which is an application centric abstraction as against having to do it at the lower layer in the cloud provider that would have required access to be managed across hundreds of resources. All access management operations are tracked and audited in an Elastic Search instance.

Logical and Physical Access Controls (CC 6.6)

The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

1	*Restricts Access—The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.*	Infrastructure is split into public and private subnets. Dev, stage, and production are split into different VPCs/VNETs. All resources by default are places in a private network and selected resources are exposed via contracts like Load balancers, Public IP. Web Application firewall protects application traffic. Host Intrusion detection is implemented via Ossec agents. Network intrusion detection is implemented via cloud provider tools like Guard Duty. The role of DuploCloud is to automatically implement them and configure all the needed configurations.
2	*Protects Identification and Authentication Credentials— Identification and authentication credentials are protected during transmission outside its system boundaries.*	Encryption at REST is done via AWS KMS/Azure KeyVault and in transit via SSL.
3	*Requires Additional Authentication or Credentials—Additional authentication information or credentials are required when accessing the system from outside its boundaries.*	DuploCloud integrates with the client's IDP like Gsuite and O365 for access to the portal. Open VPN has MFA enabled.
4	*Implements Boundary Protection Systems—Boundary protection systems (for example, firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.*	Infrastructure is split into public and private subnets. Dev, stage, and production are split into different VPCs/VNETs. All resources by default are places in a private network and selected resources are exposd via contructs like Loadbalancers, Public IP. Web Application firewall protects application traffic. Host Intrusion detection is implemented via Ossec agents. Network intrusion detection is implemented via cloud provider tools like Guarduty. The role of DuploCloud is to automatically implement them and wire all the needed configurations.

Logical and Physical Access Controls (CC 6.7)

The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

1	*Restricts the Ability to Perform Transmission—Data loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement and removal of information.*	DuploCloud by default orchestrates appropriate services like Encryption at rest and transit to protect data integrity.
2	*Uses Encryption Technologies or Secure Communication Channels to Protect Data— Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points.*	Encryption at REST is done via AWS KMS/Azure KeyVault and in transit via SSL certs.

Logical and Physical Access Controls (CC 6.8)

The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

1	*Restricts Application and Software Installation – The ability to install applications and software is restricted to authorized individuals.*	Most organizations deploy software via containers. In that scenario hosts are tightly locked, and no software is installed there beyond security software implemented by DuploCloud. Through the DuploCloud portal application deployment is enabled but any installs into host are blocked.
2	*Detects Unauthorized Changes to Software and Configuration Parameters—Processes are in place to detect changes to software and configuration parameters that may be indicative of unauthorized or malicious software.*	DuploCloud implements Ossec and ClamAV agent in the hosts. The logs from the same are collected and centralized in a SIEM which detect malicious and unauthorized activity and alert.
3	*Uses a Defined Change Control Process—A managementdefined change control process is used for the implementation of software.*	DuploCloud provides a low-code Terraform module that enables users to easily adopt infrastructure-as-code that comes with an inherent mechanism for change control.
4	*Uses Antivirus and Anti- Malware Software—Antivirus and anti-malware software is implemented and maintained to provide for the interception or detection and remediation of malware.*	DuploCloud enables ClamAV deployment via agent modules and alerts are collected and notified in a SIEM.
5	*Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software—Procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software and to remove any items detected prior to its implementation on the network.*	DuploCloud enables ClamAV deployment via agent modules and alerts are collected in Wazuh.

System Operations (CC 7.1)

To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

2	*Monitors Infrastructure and Software—The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.*	DuploCloud implements multiple layers and aspects of monitoring. Elastic Search is implemented for central logging which is configured for alerts using text patterns. CloudWatch, Azure monitoring, Prometheus and Grafana are used for monitoring infrastructure metrics. Various security monitoring is achieved by enabling Cloud trail, AWS config, OSSEC, ClamAV, etc. and the results centralized in a SIEM solution. This includes various checks like FIM, IDS, SCA, CIS Benchmarking, etc.
3	*Implements Change-Detection Mechanisms—The IT system includes a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.*	DuploCloud implements multiple layers and aspects of monitoring. Elastic Search is implemented for central logging which is configured for alerts using text patterns. CloudWatch, Azure monitoring, Prometheus and Grafana are used for monitoring infrastructure metrics. Various security monitoring is achieved by enabling Cloud trail, AWS config, OSSEC, ClamAV, etc. and the results centralized in a SIEM solution. This includes various checks like FIM, IDS, SCA, CIS Benchmarking, etc.
4	*Detects Unknown or Unauthorized Components— Procedures are in place to detect the introduction of unknown or unauthorized components.*	Various security monitoring is achieved by enabling Cloud Trail, AWS config, OSSEC, ClamAV, etc. and the results centralized in a SIEM solution. This includes various checks like FIM, IDS, SCA, CIS Benchmarking, etc.
5	*Conducts Vulnerability Scans— The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.*	Ossec agents are implemented for Vulnerability Detection. results are centralized in a SIEM.

System Operations (CC 7.2)

The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

1	*Implements Detection Policies, Procedures, and Tools— Detection policies and procedures are defined and implemented, and detection tools are implemented on Infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities.*	DuploCloud implements multiple layers and aspects of monitoring. Elastic Search is implemented for central logging which is configured for alerts using text patterns. CloudWatch, Azure monitoring, Prometheus and Grafana are used for monitoring infrastructure metrics. Various security monitoring is achieved by enabling Cloud trail, AWS config, OSSEC, ClamAV, etc. and the results centralized in a SIEM solution. This includes various checks like FIM, IDS, SCA, CIS Benchmarking, analyzing syslog's etc.

2	*Designs Detection Measures— Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software.*	DuploCloud implements multiple layers and aspects of monitoring, detection, and alerting. Elastic Search is implemented for central logging which is configured for alerts using text patterns. CloudWatch, Azure monitoring, Prometheus and Grafana are used for monitoring infrastructure metrics. Various security monitoring is achieved by enabling Cloud trail, AWS config, OSSEC, ClamAV, etc. and the results centralized in a SIEM solution. This includes various checks like FIM, IDS, SCA, CIS Benchmarking, analyzing syslog's etc.
3	*Implements Filters to Analyze Anomalies— Management has implemented procedures to filter, summarize, and analyze anomalies to identify security events.*	DuploCloud platform includes a SIEM software that enables this
4	*Monitors Detection Tools for Effective Operation— Management has implemented processes to monitor the effectiveness of detection tools.*	DuploCloud implements multiple tools that can monitor the same resources and systems. this enables monitoring of detection tools. An example of this is implementation of both OSSEC agent as well as AWS inspector. But this functionality can cause added cost and hence is not enabled by default.

System Operations (CC 7.3)

The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

1	*Responds to Security Incidents—Procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures on a periodic basis.*	DuploCloud's overall management platform which includes the SIEM enables operations team to have this evaluation procedure periodically and substantially reduces the man hours required for the process.
2	*Communicates and Reviews Detected Security Events— Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.*	DuploCloud's overall management platform which includes the SIEM enables operations team to have this evaluation procedure periodically and substantially reduces the man hours required for the process.
3	*Develops and Implements Procedures to Analyze Security Incidents—Procedures are in place to analyze security incidents and determine system impact.*	The DuploCloud policy model that provides an application centric abstraction of the infrastructure makes overall DevSecOps process to be far more efficient, requiring less subject matter expertise and reduces error. Combining this with user roles, security tools, SIEM and other aspects of infrastructure that are orchestrated, the system gives an out-ofbox DevOps-as-a-service experience. The overall surface area that needs to be dealt with humanly has been reduced substantially allowing such processes to be implemented easily.
4	*Assesses the Impact on Personal Information— Detected security events are evaluated to determine whether they could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws or regulations.*	The DuploCloud policy model that provides an application centric abstraction of the infrastructure makes overall DevSecOps process to be far more efficient, requiring less subject matter expertise and reduces error. Combining this with user roles, security tools, SIEM and other aspects of infrastructure that are orchestrated, the system gives an out-ofbox DevOps-as-a-service experience. The overall surface area that needs to be dealt with humanly has been reduced substantially allowing such processes to be implemented easily.

System Operations (CC 7.4)

The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

1	*Assigns Roles and Responsibilities— Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned, including the use of external resources when necessary.*	DuploCloud access control provides an application specific abstraction on top of low level infra resources. Users can be assigned to tenants. In addition, there are roles for security admin and auditors. Together it provides a substantially easier operating model rather than dealing with the same at the cloud provider level.
2	*Contains Security Incidents— Procedures are in place to contain security incidents that actively threaten entity objectives,*	DuploCloud platform combines both provisioning as well as detection into a single system with a single policy model. This makes building procedures for both detection and mitigation seamless for the operator. The platform delivers a DevSecOps-as-a-service solution.
3	*Mitigates Ongoing Security Incidents— Procedures are in place to mitigate the effects of ongoing security incidents.*	DuploCloud platform combines both provisioning as well as detection into a single system with a single policy model. This makes building procedures for both detection and mitigation seamless for the operator. The platform delivers a DevSecOps-as-a-service solution.
4	*Ends Threats Posed by Security Incidents— Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.*	DuploCloud platform combines both provisioning as well as detection into a single system with a single policy model. This makes building procedures for both detection and mitigation seamless for the operator. The platform delivers a DevSecOps-as-a-service solution.
5	*Restores Operations— Procedures are in place to restore data and business operations to an interim state that permits the achievement of entity objectives.*	DuploCloud platform combines both provisioning as well as detection into a single system with a single policy model. This makes building procedures for both detection and mitigation seamless for the operator. The platform delivers a DevSecOps-as-a-service solution.
6	*DuploCloud platform combines both provisioning as well as detection into a single system with a single policy model. This makes building procedures for both detection and mitigation seamless for the operator. The platform delivers a DevSecOps-as-a-service solution.*	DuploCloud platform combines both provisioning as well as detection into a single system with a single policy model. This makes building procedures for both detection and mitigation seamless for the operator. The platform delivers a DevSecOps-as-a-service solution.
7	*Obtains Understanding of Nature of Incident and Determines Containment Strategy—An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.*	DuploCloud platform combines both provisioning as well as detection into a single system with a single policy model. This makes building procedures for both detection and mitigation seamless for the operator. The platform delivers a DevSecOps-as-a-service solution.

8	*Remediates Identified Vulnerabilities—Identified vulnerabilities are remediated through the development and execution of remediation activities.*	Remediation is done by swapping out new hardened images with old ones. DuploCloud platform orchestrates this process at scale across the infrastructure with simple declarative triggers like updates per environment, built in state machines for zero downtime upgrades etc.
9	*Mitigates Ongoing Security Incidents—Procedures are in place to mitigate the effects of ongoing security incidents.*	DuploCloud platform combines both provisioning as well as detection into a single system with a single policy model. This makes building procedures for both detection and mitigation seamless for the operator. The platform delivers a DevSecOps-as-a-service solution.
10	*Evaluates the Effectiveness of Incident Response—The design of incident response activities is evaluated for effectiveness on a periodic basis.*	DuploCloud access control provides an application specific abstraction on top of low level infra resources. Users can be assigned to tenants. In addition, there are roles for security admin and auditors. Together it provides a substantially easier operating model rather than dealing with the same at the cloud provider level.
11	*Periodically Evaluates Incidents—Periodically, management reviews incidents related to security, availability, processing integrity, confidentiality, and privacy and identifies the need for system changes based on incident patterns and root causes.*	DuploCloud access control provides an application specific abstraction on top of low level infra resources. Users can be assigned to tenants. In addition, there are roles for security admin and auditors. Together it provides a substantially easier operating model rather than dealing with the same at the cloud provider level.
12	*Application of Sanctions—The conduct of individuals and organizations operating under the authority of the entity and involved in the unauthorized use or disclosure of personal information is evaluated and, if appropriate, sanctioned in accordance with entity policies and legal and regulatory requirements.*	DuploCloud's auditor role logs user actions in application context which makes putting the user actions in the context of easy to understand business context and thus facilitates the process.

System Operations (CC 7.5)

The entity identifies, develops, and implements activities to recover from identified security incidents.

1	*Restores the Affected Environment—The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed.*	DuploCloud platform combines both provisioning as well as detection into a single system with a single policy model. this makes building procedures for both detection and mitigation seamless for the operator. The platform delivers a DevSecOps-as-a-service solution.
6	*Implements Incident Recovery Plan Testing—Incident recovery plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans, and systems based on test results.*	DuploCloud provides a low-code approach that makes adoption of infrastructure-as-code easy. Much of the code is auto generated. Adoption of IAC brings in inherent advantages for the incident recovery plan.

Change Management (CC 8.1)

The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

1	*Manages Changes Throughout the System Lifecycle—A process for managing system changes throughout the lifecycle of the system and its components (infrastructure, data, software and procedures) is used to support system availability and processing integrity.*	DuploCloud provides a low-code approach that makes adoption of infrastructure-as-code easy. Much of the code is auto generated. Adoption of IAC brings in inherent advantages for the incident recovery plan.
2	*Authorizes Changes—A process is in place to authorize system changes prior to development.*	DuploCloud provides a low-code approach that makes adoption of infrastructure-as-code easy. Much of the code is auto-generated. Adoption of IAC brings in its inherent advantages and implementation of change management. In this case the Code review is the process to authorize system changes. The same code review with native cloud provider IAC would have been very laborious and require substantial subject matter expertise.
3	*Designs and Develops Changes—A process is in place to design and develop system changes.*	DuploCloud provides a low-code approach that makes adoption of infrastructure-as-code easy. Much of the code is auto-generated. Adoption of IAC brings in its inherent advantages and implementation of change management. In this case the Code review is the process to authorize system changes. The same code review with native cloud provider IAC would have been very laborious and require substantial subject matter expertise.
4	*Documents Changes—A process is in place to document system changes to support ongoing maintenance of the system and to support system users in performing their responsibilities.*	DuploCloud provides a low-code approach that makes adoption of infrastructure-as-code easy. Much of the code is auto generated. Adoption of IAC acts as the de facto documentation of changes.
5	*Tracks System Changes—A process is in place to track system changes prior to implementation.*	DuploCloud provides a low-code approach that makes adoption of infrastructure-as-code easy. Much of the code is auto generated. Adoption of IAC acts as the de facto change tracking system.
6	*Configures Software—A process is in place to select and implement the configuration parameters used to control the functionality of software.*	DuploCloud provides a low-code approach that makes adoption of infrastructure-as-code easy. Much of the code is auto generated. Adoption of IAC comes with default configuration parameters.
7	*Tests System Changes—A process is in place to test system changes prior to implementation.*	DuploCloud Tenants provide the functionality to replicate and test changes in isolated ephemeral environments.
8	*Approves System Changes—A process is in place to approve system changes prior to implementation.*	DuploCloud provides a low-code approach that makes adoption of infrastructure-as-code easy. Much of the code is auto generated. Adoption of IAC comes with a de facto approval process.
9	*Deploys System Changes—A process is in place to implement system changes.*	DuploCloud provides a low-code approach that makes adoption of infrastructure-as-code easy. Much of the code is auto generated. Adoption of IAC comes with a de facto process to do the same.

10	*Identifies and Evaluates System Changes—Objectives affected by system changes are identified, and the ability of the modified system to meet the objectives is evaluated throughout the system development life cycle.*	DuploCloud provides a low-code approach that makes adoption of infrastructure-as-code easy. Much of the code is auto generated. Adoption of IAC comes with a de facto process to do the same.
11	*Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents—Changes in infrastructure, data, software, and procedures required to remediate incidents to continue to meet objectives are identified, and the change process is initiated upon identification.*	DuploCloud provides a low-code approach that makes adoption of infrastructure-as-code easy. Much of the code is auto generated. Adoption of IAC comes with a de facto process to do the same.
12	*Creates Baseline Configuration of IT Technology—A baseline configuration of IT and control systems is created and maintained.*	DuploCloud provides a low-code approach that makes adoption of infrastructure-as-code easy. Much of the code is auto generated. Adoption of IAC comes with a de facto process to do the same.
13	*Provides for Changes Necessary in Emergency Situations —A process is in place for authorizing, designing, testing, approving and implementing changes necessary in emergency situations (that is, changes that need to be implemented in an urgent timeframe).*	DuploCloud provides a low-code approach that makes adoption of infrastructure-as-code easy. Much of the code is auto generated. Adoption of IAC comes with a de facto process to do the same.
14	*Protects Confidential Information—The entity protects confidential information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to confidentiality.*	DuploCloud provides a low-code approach that makes adoption of infrastructure-as-code easy. Much of the code is auto generated. Adoption of IAC comes with a de facto process to do the same.
15	*Protects Personal Information—The entity protects personal information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to privacy.*	DuploCloud provides a low-code approach that makes adoption of infrastructure-as-code easy. Much of the code is auto generated. Adoption of IAC comes with a de facto process to do the same.

Additional Criteria for Availability (A 1.1)

The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

1	*Measures Current Usage—The use of the system components is measured to establish a baseline for capacity management and to use when evaluating the risk of impaired availability due to capacity constraints.*	DuploCloud implements multiple layers and aspects of monitoring. Elastic Search is implemented for central logging which is configured for alerts using text patterns. CloudWatch, Azure monitoring, Prometheus and Grafana are used for monitoring infrastructure metrics. Alerts can be setup easily based off these metrics and are exposed in an application specific context.
2	*Forecasts Capacity—The expected average and peak use of system components is forecasted and compared to system capacity and associated tolerances. Forecasting considers capacity in the event of the failure of system components that constrain capacity.*	DuploCloud implements multiple layers and aspects of monitoring. Elastic Search is implemented for central logging which is configured for alerts using text patterns. CloudWatch, Azure monitoring, Prometheus and Grafana are used for monitoring infrastructure metrics. Evaluating historic trends in an out-of-box metric, provides the ability to forecast accurately.
3	*Makes Changes Based on Forecasts—The system change management process is initiated when forecasted usage exceeds capacity tolerances.*	DuploCloud is both a provisioning as well as a monitoring tool providing a DevOps-as-aservice experience. Changes can be easily implemented via a no-code UI or low-code Terraform.

Additional Criteria for Availability (A 1.2)

The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

5	*Responds to Environmental Threat Events—Procedures are in place for responding to environmental threat events and for evaluating the effectiveness of those policies and procedures on a periodic basis. This includes automatic mitigation systems (for example, uninterruptable power system and generator back-up subsystem).*	DuploCloud infrastructure is created with 2 or more availability zones (azs). This alternate storage and processing capability provides transfer and resumption of system operation in times of failure.
8	*Performs Data Backup— Procedures are in place for backing up data, monitoring to detect back-up failures, and initiating corrective action when such failures occur.*	DuploCloud implements out-of-box backup procedures for database, file shares, Elastic Search, and configuration. DuploCloud accomplishes this with a single click versus creating onerous of scripts.
9	*Addresses Offsite Storage— Back-up data is stored in a location at a distance from its principal storage location sufficient that the likelihood of a security or environmental threat event affecting both sets of data is reduced to an appropriate level.*	DuploCloud's Infrastructure concept captures the notion of regions, and this provide the needed abstraction to implement a multiregion backup.
10	*Implements Alternate Processing Infrastructure— Measures are implemented for migrating processing to alternate infrastructure in the event normal processing infrastructure becomes unavailable.*	DuploCloud's Infrastructure concept captures the notion of regions, and this provide the needed abstraction to implement a multiregion environment.

Additional Criteria for Availability (A 1.3)

The entity tests recovery plan procedures supporting system recovery to meet its objectives.

1	*Implements Business Continuity Plan Testing— Business continuity plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.*	DuploCloud's Infrastructure concept captures the notion of regions, and this provide the needed abstraction to implement a multiregion environment. Further using the low-code Infrastructure as code technique, environments can be replicated easily.
2	*Tests Integrity and Completeness of Back-Up Data—The integrity and completeness of back-up information is tested on a periodic basis.*	DuploCloud's Infrastructure concept captures the notion of regions, and this provide the needed abstraction to implement a multiregion environment. Further using the low-code Infrastructure as code technique, environments can be replicated easily.

Additional Criteria for Confidentiality (C 1.1)

The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.

5	*Identifies Confidential information— Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.*	DuploCloud abstraction of tenants comes with the ability to label data. By adding simple labels at tenant levels and resource levels, DuploCloud implicitly propagates these labels down to cloud resources
8	*Protects Confidential Information from Destruction—Procedures are in place to protect confidential information from erasure or destruction during the specified retention period of the information.*	

Additional Criteria for Processing Integrity and Privacy

DuploCloud does not collect or store customer data.