

# **Out-of-the-Box Compliance with a No-Code & Low-Code DevOps Platform**



# **DuploCloud**

---

## TABLE OF CONTENTS

INTRODUCTION	3
DUPLOCloud APPROACH	5
SELF-HOSTED	6
POLICY MODEL	6
<i>Agent Modules</i>	8
PREREQUISITE READING	9
SECURITY INFORMATION AND EVENT MANAGEMENT	9
PCI DSS - SUPER SET OF STANDARDS	11
PROVISIONING TIME CONTROLS (DEVOPS)	11
<i>Network, Security and IAM (Requirement 1)</i>	11
<i>Secret Management (Requirement 2)</i>	13
<i>Encryption and Key Management (Requirement 3)</i>	15
<i>Transport Encryption (Requirement 4)</i>	16
<i>Access Control (Requirements 7 &amp; 8)</i>	17
POST PROVISIONING CONTROLS (SECOPS)	22
<i>Vulnerability Detection (Requirement 6.1)</i>	22
<i>CIS Benchmarks (Requirement 1)</i>	23
<i>Cloud Vulnerabilities &amp; Intrusion Detection (Requirement 11.4)</i>	24
<i>File Integrity Monitoring (Requirement 10.5.5)</i>	26
<i>Virus Scanning (Requirements 5.1, 5.2 &amp; 5.3)</i>	27
<i>Network Intrusion Detection (Requirement 11.4)</i>	28
<i>Inventory Management (Requirement 11)</i>	30
<i>Host Intrusion Detection (Requirement 10.6.1)</i>	31
<i>Host Anomaly Detection</i>	32
<i>Email Alerting</i>	33
<i>Incident Management</i>	33
CONTROL-BY-CONTROL PCI IMPLEMENTATION DETAIL	34
<i>Control-by-Control HIPAA Implementation Detail</i>	51

---

## Introduction

Businesses operating in regulated industries are required to abide by a set of guidelines set forth by standard bodies in their respective industries. For example, the Payment Card Industry (PCI) has defined Data Security Standard (DSS), and Health Care has defined HIPAA and HITRUST. SOC-2 is a more generic standard that is widely used in a broad set of industries. There are also guidelines based on the region of operations, such as GDPR. These guidelines, called “controls” are split into IT and non-IT functions (i.e., HR, Finance, Legal). IT controls are split into the following categories:

1. **Controls implemented by Cloud Provider.** Items such as physical datacenter, host virtualization, management software and services provided by the cloud providers. AWS, Azure and GCP meet virtually all the standards and their certifications are readily available for download from their webpages.
2. **Controls to be implemented by the Organization's Cloud Ops Team.** *These pertain to how various cloud provider services are consumed and configured by the organization hosting their application on the cloud. The cloud providers themselves are not responsible for this but do provide a prescriptive set of guidelines on how to implement various controls using their services, community and third-party commercial software available in their marketplace. For example,*  
<https://docs.aws.amazon.com/config/latest/developerguide/operational-best-practices-for-pci-dss.html>
3. **Controls to be implemented by the Organization's product team.** Like infrastructure controls, there are a set of guidelines around software development and release procedures that need to be followed by the product development team.
4. **Controls to be implemented in Organization's User Device Management Team.** These are controls around the use and safety of user devices like company laptops and mobile phones.

The document focuses on Number 2 above and describes the DuploCloud Implementation of various controls. Also provided is an implementation matrix mapping the respective compliance standards to the DuploCloud Implementation.

*It is a common misconception that if the cloud provider is meeting a certain compliance guideline, say SOC-2, the organization hosting the application on the provider is automatically fully certified. The cloud is a shared security model, the consumers are responsible to configure the service provided by the cloud vendor to match their 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 hosting organization.*

---

## DuploCloud Approach

DuploCloud is a DevSecOps software platform which builds and operates a fully compliant infrastructure on your behalf based on the standard of your choice.

*DuploCloud is a no-code solution which performs the stitching function underneath DevOps, 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, ClamAV for antivirus, and Suricata for NIDS. Finally, for remaining controls or based on customer preference for a certain tool, the framework integrates third-party ISV tools. This extensibility is available user-added 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 (like PCI, HIPAA, SOC-2)
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. Users 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 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-or-internet 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/installclamavcron.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>

More information is available @ [www.duplocloud.com](http://www.duplocloud.com)

## Security Information and Event Management

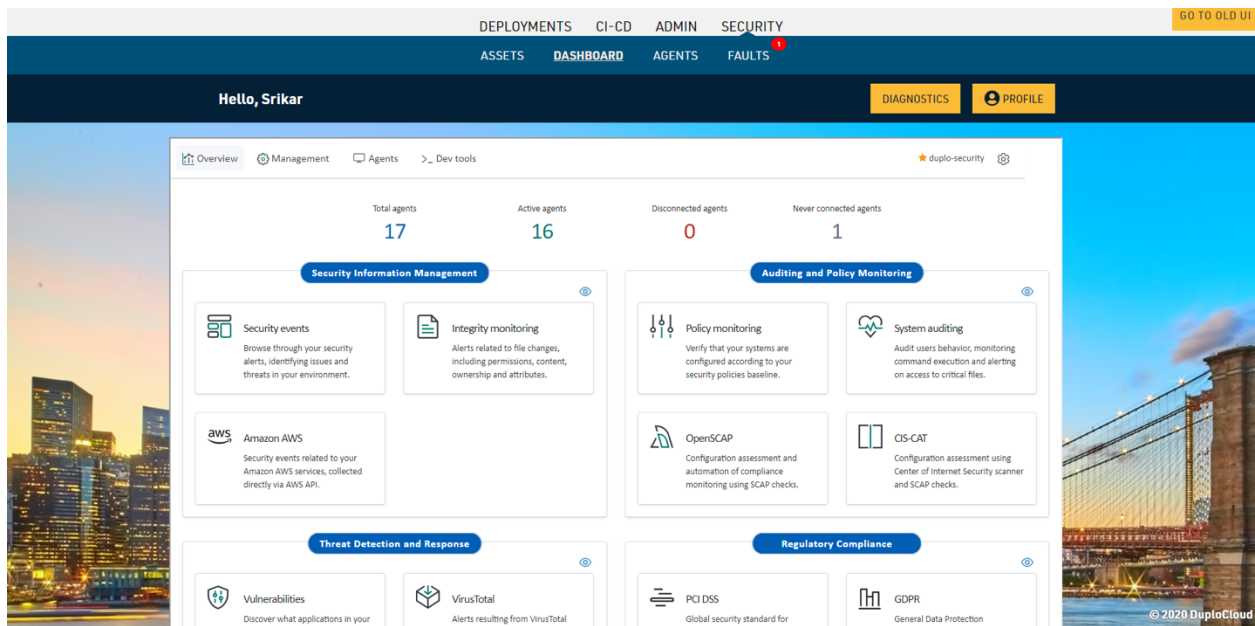
Every infrastructure has a centralized system to aggregate and process all events. The primary functions of the system are:

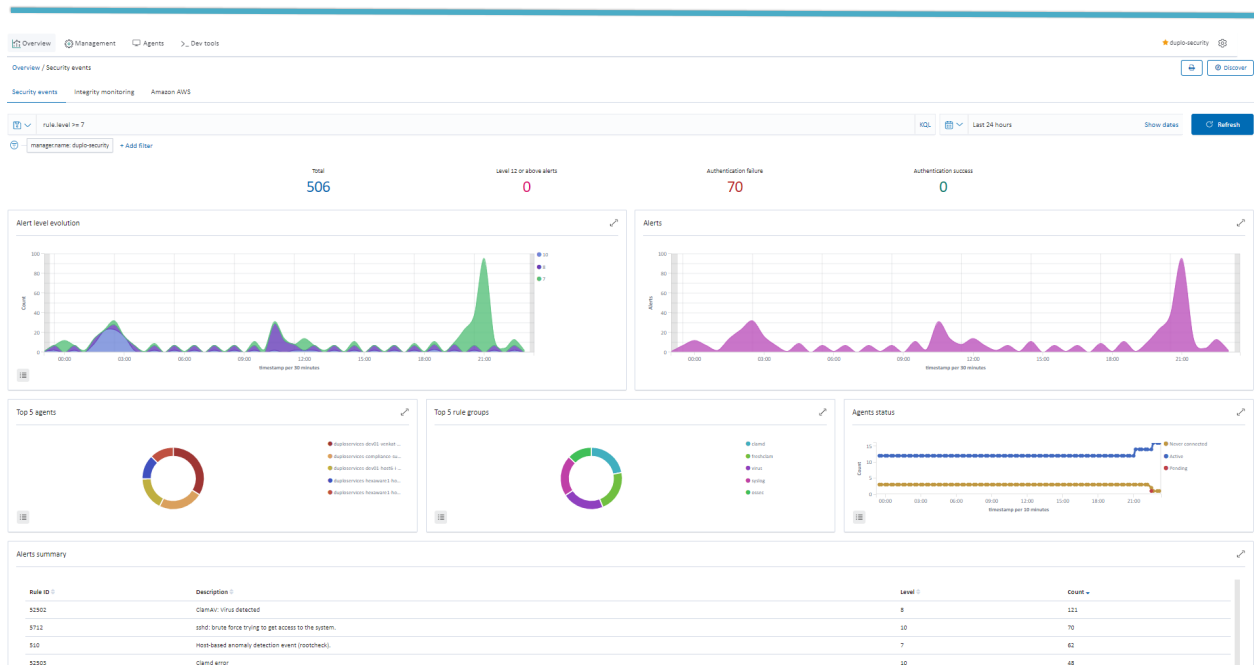
1. Data Repository
2. Event Processing Rules
3. Dashboard
4. Events and Alerting



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 PCI DSS implementation in the Wazuh dashboard.





## PCI DSS - Super set of standards

The security guidelines from various standards have a large overlap. Some guidelines are more stringent than others, with PCI DSS and HITRUST the most stringent. Their controls are a super set of controls from most other standards, specifically SOC-2, GDPR and HIPAA. This document describes the controls implemented by DuploCloud mapping to PCI DSS, which subsume SOC-2, GDPR, HIPAA and HITRUST. The controls matrix at the end provides the mapping with PCI-DSS and HIPAA.

## Provisioning Time Controls (DevOps)

### Network, Security and IAM (Requirement 1)

	PCI DSS Requirements v3.2.1	DuploCloud Implementation
Requirement 1: Install and maintain a firewall configuration to protect cardholder data		
1.	1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the Internal network zone	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.
2.	1.1.5 Description of groups, roles, and responsibilities for management of network components.	DuploCloud overlays logical constructs of Tenant and infrastructure that represents an application. Within a tenant there are concepts of services. All resources within the tenant are by default labeled in the cloud with the Tenant name. Further the automation allows the user to set any tag at a tenant level and that is automatically propagated to AWS/Azure artifacts. The system is always kept in sync with background threads
3.	1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	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.
4.	1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	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.
5.	1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	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.

6.	1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	By default, all outbound traffic uses NAT Gateway. We can put in place additional subnet ACLs if needed. Nodes in the private subnets can only go outside only via a NAT Gateway. In Azure outbound can be blocked in the VNET
7.	1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	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 frontend UI is in a different tenant
8.	1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties.	Use Private subnets and private R53 hosted zones/Private Azure DNS zones
9.	1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties	Usage of a rules-based approach makes the configuration error free, consistent and documented. Further documentation is to be done by the client and we also put in documentation during the blue printing process

## Secret Management (Requirement 2)

	PCI DSS Requirements v3.2.1	DuploCloud Implementation
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters		
1.	2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems,	DuploCloud enables user specified password or random password generation options. User access is managed in such a way that all end user access is via single sign on and password less. Even access to AWS/Azure console is done by generating a federated console URL that has a validity of less than an hour. The system enables operations with minimal user accounts as most access is JIT

	software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.)	
2.	<p>2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)</p> <p>Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.</p>	DuploCloud orchestrates K8 node selectors for this and supports non container workloads and allows labeling of VMs and achieving this. For non-container workloads are also supported and hence allows automation to meet these controls. For example, one can install Wazuh in one VM, Suricata in another and Elastic Search in another
3.	2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	By default, no traffic is allowed inside a tenant boundary unless exposed via an LB. DuploCloud allows automated configuration of desired inter-tenant access w/o users needing to manually write scripts. Further as the env changes dynamically DuploCloud keys these configs in sync. DuploCloud also reconciles any orphan resources in the system and cleans them up, this includes docker containers, VMs, LBs, keys, S3 buckets and various other resources
4.	<p>2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.</p> <p>Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.</p>	DC gets certificates from Cert-Manager and automates SSL termination in the LB
5.	2.2.4 Configure system security parameters to prevent misuse.	IAM configuration and policies in AWS/ Managed Identities in Azure that implement separation of duties and least privilege, S3 bucket policies. 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 frontend UI is in a different tenant
6.	2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	DuploCloud reconciles any orphan resources in the system against the user specifications in its database and cleans them up, this includes docker containers, VMs, LBs, keys, S3 buckets and various other resources. All resources specified by the user in the database are tracked and audited every 30 seconds
7.	2.3 Encrypt all non-console administrative access using strong cryptography.	SSL LB and VPN connections are orchestrated. DuploCloud automates OpenVPN P2S VPN user management by integrating it with user's single sign on i.e., when a user's email is revoked from DuploCloud portal, it is cleaned up automatically from the VPN server
8.	2.4 Maintain an inventory of system components that are in scope for PCI DSS.	All resources are stored in DB, tracked, and audited. The software has an inventory of resources that can be exported

## Encryption and Key Management (Requirement 3)

	PCI DSS Requirements v3.2.1	DuploCloud Implementation
Requirement 3: Protect stored cardholder data		
1.	3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must	DuploCloud orchestrates AWS KMS/Azure Key Vault keys per tenant to encrypt various AWS/Azure resources 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

	<p>not be associated with user accounts.</p> <p>Note: This requirement applies in addition to all other PCI DSS encryption and key-management requirements.</p>	
2.	3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.	DuploCloud orchestrates AWS KMS/Azure Key Vault keys per tenant to encrypt various AWS/Azure resources 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
3.	<p>3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:</p> <ul style="list-style-type: none"> <li>• Encrypted with a key-encrypting key that is at least as strong as the data encrypting key, and that is stored separately from the data-encrypting key</li> <li>• Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device)</li> <li>• As at least two full-length key components or key shares, in accordance with an industry accepted method</li> </ul> <p>Note: It is not required that public keys be stored in one of these forms.</p>	DuploCloud orchestrates AWS KMS/Azure KeyVault for this and that in turns provides this control that we inherit

## Transport Encryption (Requirement 4)

	PCI DSS Requirements v3.2.1	DuploCloud Implementation
Requirement 4: Encrypt transmission of cardholder data across open, public networks		

1.	<p>4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:</p> <ul style="list-style-type: none"> <li>• Only trusted keys and certificates are accepted.</li> <li>• The protocol in use only supports secure versions or configurations.</li> <li>• The encryption strength is appropriate for the encryption methodology in use.</li> </ul> <p>Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed. Examples of open, public networks include but are not limited to:</p> <ul style="list-style-type: none"> <li>• The Internet</li> <li>• Wireless technologies, including 802.11 and Bluetooth</li> <li>• Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)</li> <li>• General Packet Radio Service (GPRS)</li> <li>• Satellite communications</li> </ul>	<p>In the secure infrastructure blueprint we adopt Application Load Balancers with HTTPS listeners. HTTP listeners forwarded to HTTPS. The latest cipher is used in the LB automatically by the DuploCloud software</p>
----	--	---

## Access Control (Requirements 7 & 8)

	PCI DSS Requirements v3.2.1	DuploCloud Implementation
Requirement 7: Restrict access to cardholder data by business need to know		
1.	<p>7.1.1 Define access needs for each role, including:</p> <ul style="list-style-type: none"> <li>• System components and data resources that each role needs to access for their job function</li> <li>• Level of privilege required (for example, user, administrator, etc.) for accessing resources</li> </ul>	<p>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 in AWS/NSG in Azure. Tenant access policies will automatically apply SG or IAM based policy in AWS/NSG, or Managed Identity in Azure based on the resource type.</p>



	7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed. This access control system(s) must include the following	User access to AWS/Azure console is granted based on tenant permissions and least privilege and a Just in time federated token that expires in less than an hour. Admins have privileged access and read-only user is another role
2.	7.2.1 Coverage of all system components.	AWS resource access is controlled based on IAM role, SG and static VPN client Ips/ Azure resource access in controlled by NSG, Managed Identity and static VPN client Ips that are all implicitly orchestrated and kept up to date
3.	7.2.3 Default deny-all setting.	This is the default DuploCloud implementation of Sg and IAM roles in AWS/NSG and Managed Identity in Azure
Requirement 8: Identify and authenticate access to system components		
4.	8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal. From there a federated logic is done for AWS/Azure resource access
5.	8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	This is done at infra level in DuploCloud portal using single sign on
6.	8.1.3 Immediately revoke access for any terminated users.	DuploCloud integrates with client's IDP like G Suite 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
7.	8.1.4 Remove/disable inactive user accounts within 90 days.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal. The moment the email is disabled all access is revoke. Even if the user has a private key to a VM even then he cannot connect because VPN will be deprovisioned
8.	8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows:	DuploCloud integrates by calling STS API to provide JIT token and URL

	<ul style="list-style-type: none"> <li>• Enabled only during the time period needed and disabled when not in use.</li> <li>• Monitored when in use.</li> </ul>	
9.	8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal. When DuploCloud managed OpenVPN is used it is setup to lock the user out after failed attempts
10.	8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal. When DuploCloud managed OpenVPN is used it is setup to lock the user out after failed attempts. In Open VPN an admin has to unlock the user
11.	8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	DuploCloud single sign on has configurable timeout. For AWS/Azure resource access we provide JIT access
12.	<p>8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:</p> <ul style="list-style-type: none"> <li>• Something you know, such as a password or passphrase</li> <li>• Something you have, such as a token device or smart card</li> <li>• Something you are, such as a biometric.</li> </ul>	DuploCloud relies on the client's single sign on / IDP. If the user secures his corporate login using these controls then by virtue of single sign on, this get implemented in the infrastructure.
13.	8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	Encryption at REST is done via AWS KMS/Azure KeyVault and in transit via SSL
14.	8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets,	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal.

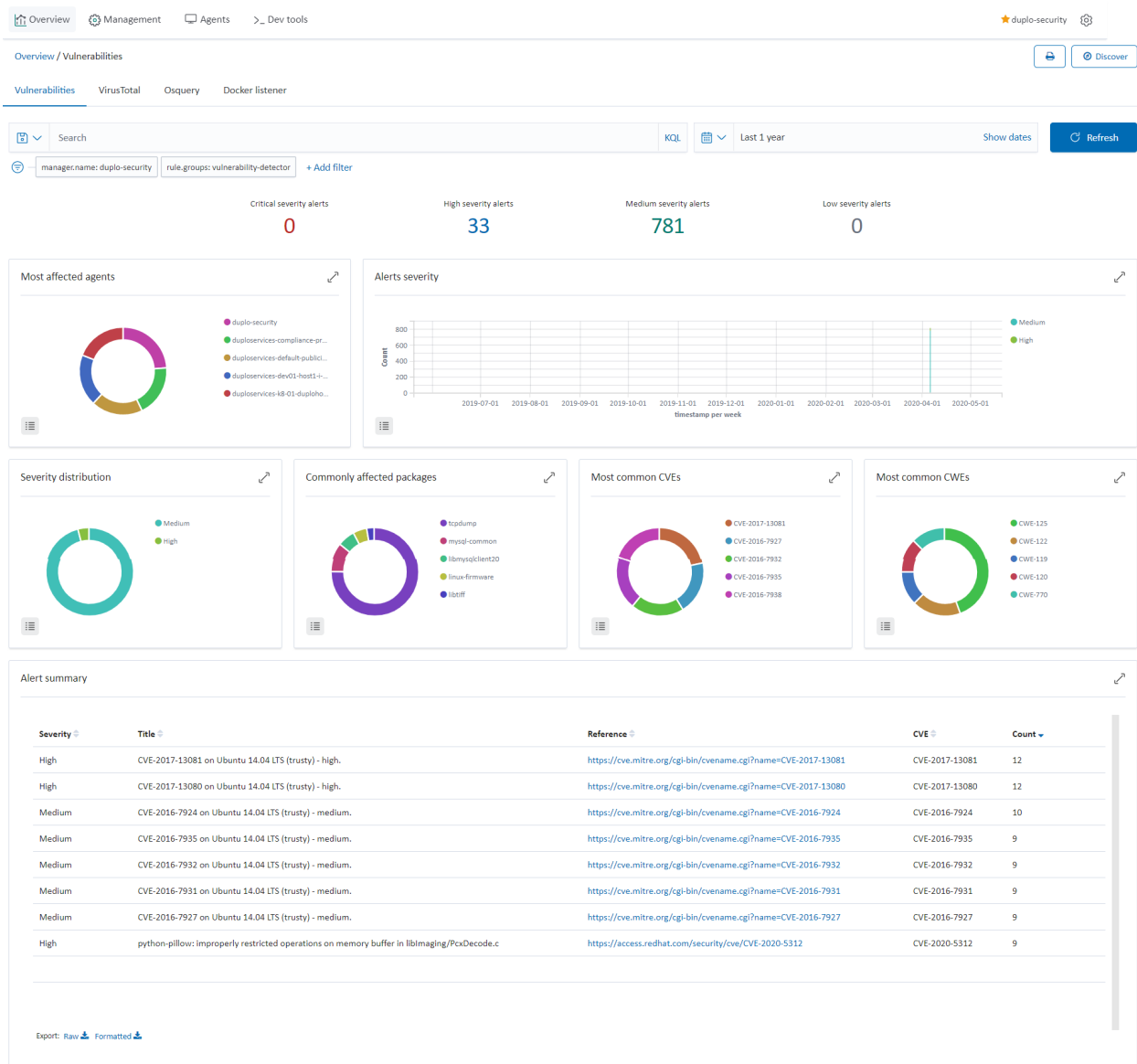
	provisioning new tokens, or generating new keys.	
15.	<p>8.2.3 Passwords/phrases must meet the following:</p> <ul style="list-style-type: none"> <li>• Require a minimum length of at least seven characters.</li> <li>• Contain both numeric and alphabetic characters.</li> </ul> <p>Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.</p>	Enforced by AWS/Azure and should be enforced by client's IDP. DuploCloud integrates with the IDP. The control should be implemented by the organization IDP.
16.	8.2.4 Change user passwords/passphrases at least every 90 days.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal.
17.	8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	Enforced by AWS/Azure and should be enforced by client's IDP. DuploCloud integrates with the IDP. The control should be implemented by the organization IDP.
18.	8.2.6 Set passwords/phrases for first time use and upon reset to a unique value for each user, and change immediately after the first use.	Enforced by AWS/Azure and should be enforced by client's IDP. DuploCloud integrates with the IDP. The control should be implemented by the organization IDP.
19.	<p>8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.</p> <p>Note: Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.</p>	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal. Open VPN has MFA enabled

20.	8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal. Open VPN has MFA enabled
21.	8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator and including third-party access for support or maintenance) originating from outside the entity's network.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal. Open VPN has MFA enabled
22.	<p>8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:</p> <ul style="list-style-type: none"> <li>• All user access to, user queries of, and user actions on databases are through programmatic methods.</li> <li>• Only database administrators can directly access or query databases.</li> <li>• Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes)</li> </ul>	The IAM integration with database makes SQL connections also via Instance Profile. For users, individual JIT access is granted that lasts only 15 mins

# Post Provisioning Controls (SecOps)

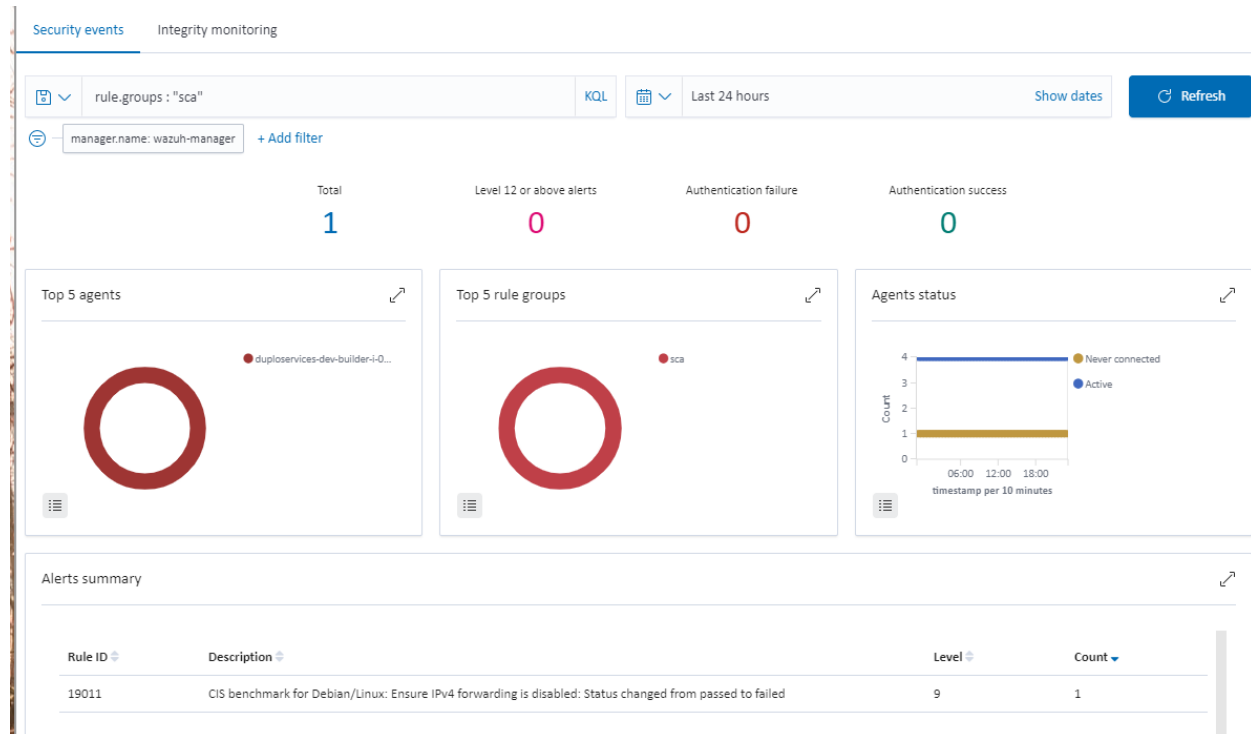
## Vulnerability Detection (Requirement 6.1)

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 (Requirement 1)

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 (Requirement 11.4)

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:

The screenshot displays the DuploCloud SIEM dashboard interface. At the top, there are navigation tabs: Overview, Management, Agents, and Dev tools. The main header shows 'Overview / Amazon AWS' with a 'Discover' button. Below this, there are filters for 'manager.name: duplo-security', 'rule.groups: amazon', and 'rule.description: AWS Cloudtrail: signin.amazonaws.com - ConsoleLogin - Possible breaking attempt (high number of login attempts)'. A search bar and a 'Refresh' button are also present.

The dashboard features four circular progress indicators for different categories: Sources (cloudtrail), Accounts (83752), S3 buckets (duplosecurity-compliance-aud...), and Regions (us-east-1). Below these, a table titled 'Top rules' shows a single rule with ID 80255, description 'AWS Cloudtrail: signin.amazonaws.com - ConsoleLogin - Possible breaking attempt (high number of login attempts)', and a count of 1.

The main content area displays a log entry for a security alert. The log entry includes the following details:

- Time: 15, 2020 @ 02:33:09.471
- manager.name: duplo-security
- rule.description: AWS Cloudtrail: signin.amazonaws.com - ConsoleLogin - Possible breaking attempt (high number of login attempts)
- rule.groups: amazon, aws, aws\_cloudtrail, authentication\_failures
- input.type: log
- agent.name: duplo-security
- agent.id: 000
- previous\_output: {"integration": "aws", "aws": {"log\_info": {"aws\_account\_alias": "", "log\_file": "cloudtrail/AWSLogs/837529338966/CloudTrail/us-east-1/2020/05/14/837529338966-CloudTrail-us-east-1\_20200514T0502\_kh190FpK001UxJP.json.gz", "s3bucket": "duplosecurity-compliance-audit-837529338966"}, "eventVersion": "1.05"}}

The log entry is displayed in a JSON format, showing the following fields:

- GeoLocation.city\_name: Tr
- GeoLocation.country\_name: India
- GeoLocation.location: {"lon": 80.5833, "lat": 16.75}
- GeoLocation.region\_name: Ar
- \_id: G3H\_FHIBMcG2nF;Fe8
- \_index: security-alerts-3.x-2020.05.14
- \_score: -
- \_type: \_doc
- agent.id: 000
- agent.name: duplo-security
- data.aws.additionalEventData.LoginTo: https://console.aws.amazon.com/console/home?state-hashArgv%5B%5Dauthcode=true
- data.aws.additionalEventData.MFAUsed: No
- data.aws.additionalEventData.MobileVersion: No
- data.aws.awsRegion: us-east-1
- data.aws.aws\_account\_id: 837529338966
- data.aws.errorMessage: Failed authentication
- data.aws.eventID: 76dd940-7130-455a-bf5e-b967d7464054
- data.aws.eventName: ConsoleLogin
- data.aws.eventSource: signin.amazonaws.com
- data.aws.eventTime: 2020-05-14T02:48:34Z
- data.aws.eventType: AwsConsoleSignIn
- data.aws.eventVersion: 1.05

```

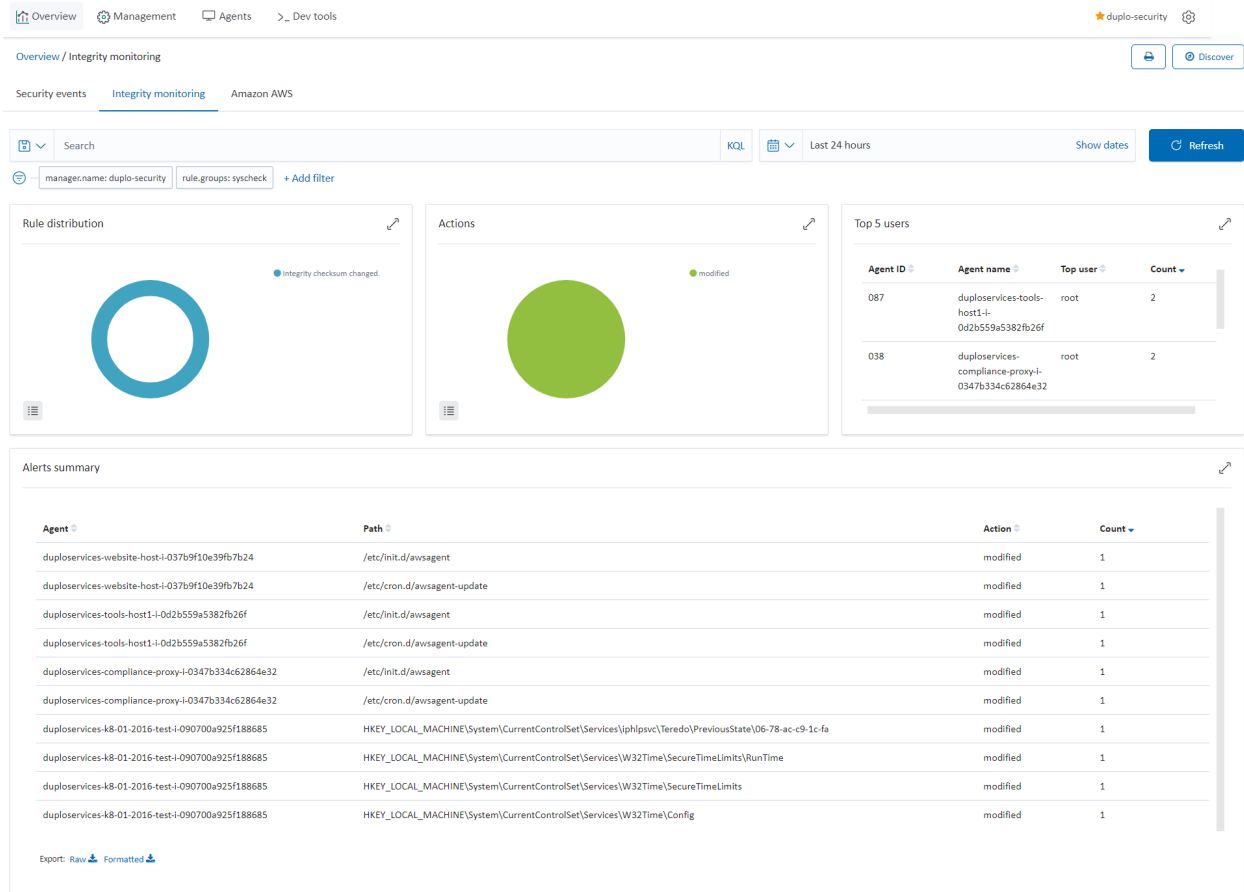
# data.aws.log.info.log.file      cloudtrail/Amazon/837529338096/CloudTrail/us-east-1/2020/05/14/837529338096_CloudTrail-us-east-1_20200514T2058Z_s3Kpp5kAb7X67N.json.gz
# data.aws.log.info.s3bucket      duplo-services-compliance-audit-837529338096
# data.aws.recipientAccountId      837529338096
# data.aws.responseElements.ConsoleLogin  failure
# data.aws.source                cloudtrail
# data.aws.sourceIPAddress        175.191.99.21
# data.aws.source_ip_address      175.191.99.21
# data.aws.userAgent              Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
# data.aws.userIdentity.accountId  837529338096
# data.aws.userIdentity.principalId AIDA6AFDCYEZTAVZERO
# data.aws.userIdentity.type       IAMUser
# data.aws.userIdentity.userName   sriker@duplocloud.net
# data.integration                aws
# decoder.name                    json
# id                              1589450185_10072163
# input.type                      log
# location                        Duplo-AWS
# manager.name                    duplo-security
# previous output                  {}
# rule.description                 AWS Cloudtrail: signin.amazonaws.com - ConsoleLogin - Possible breaking attempt (high number of login attempts)
# rule.firetimes                  1
# rule.frequency                   6
# rule.gdpr                       IV_35.7.d, IV_32.2
# rule.groups                      aws, aws_cloudtrail, authentication_failures
# rule.hipaa                      164.312.b
# rule.id                         86255
# rule.level                       10
# rule.mail                        false
# rule.nist_800_53                 SI.4, AU.14, AC.7
# rule.pci_dss                    11.4, 10.2.4, 10.2.5
# timestamp                       May 15, 2020 @ 02:33:09.471

```



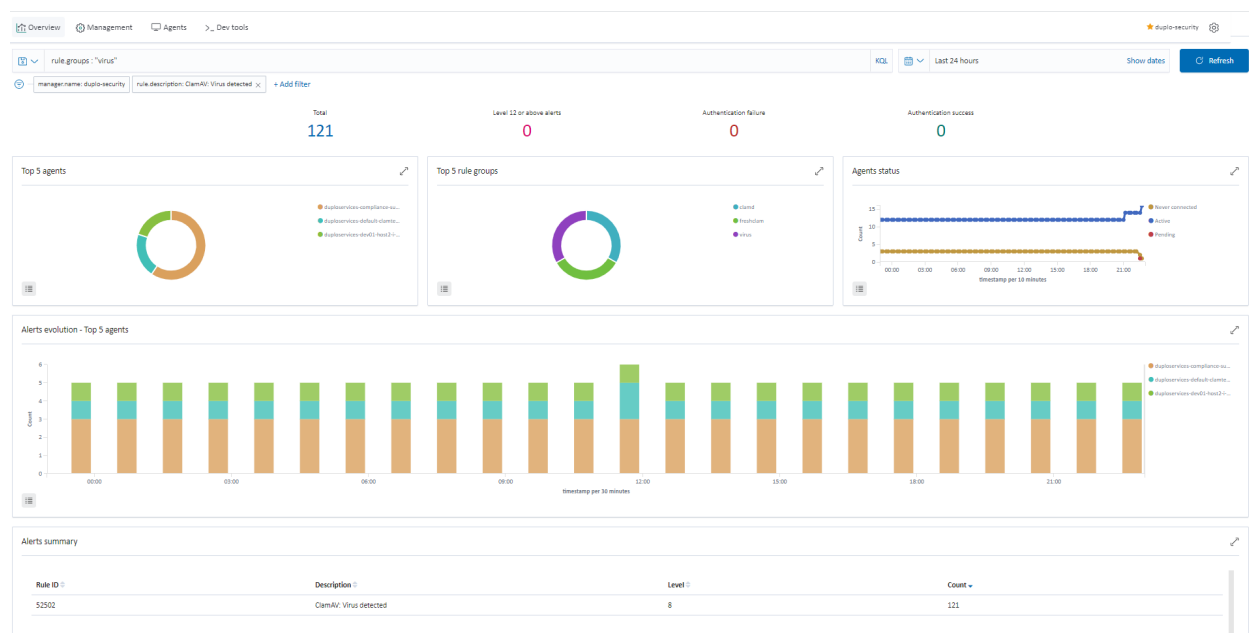
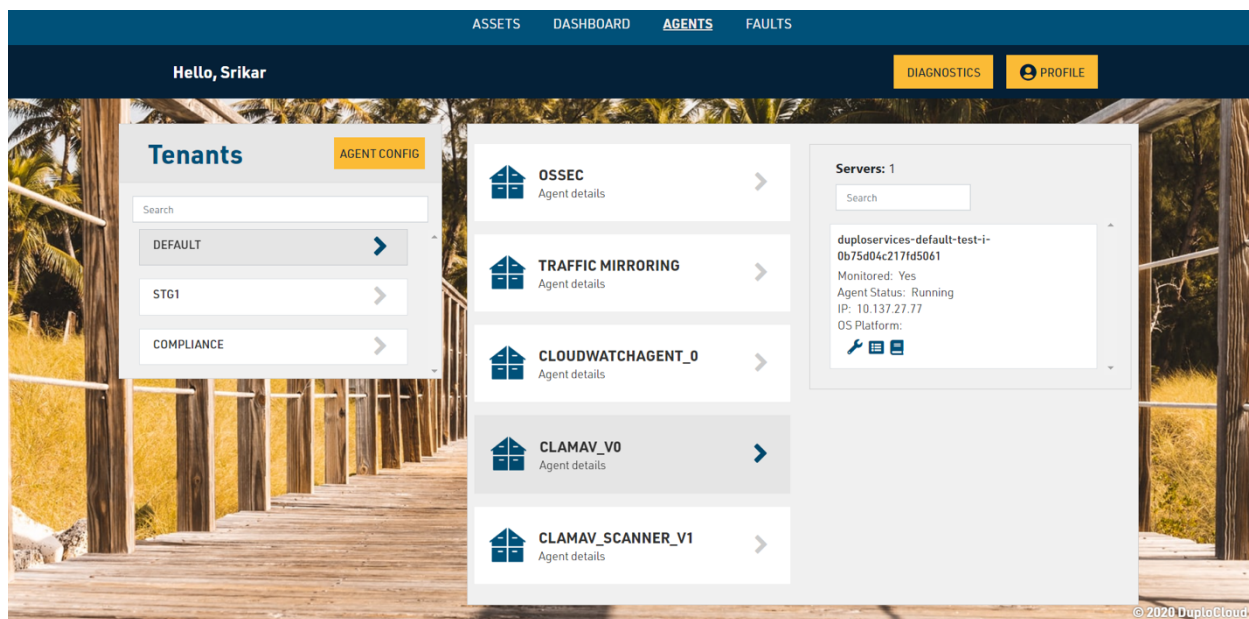
## File Integrity Monitoring (Requirement 10.5.5)

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](#).



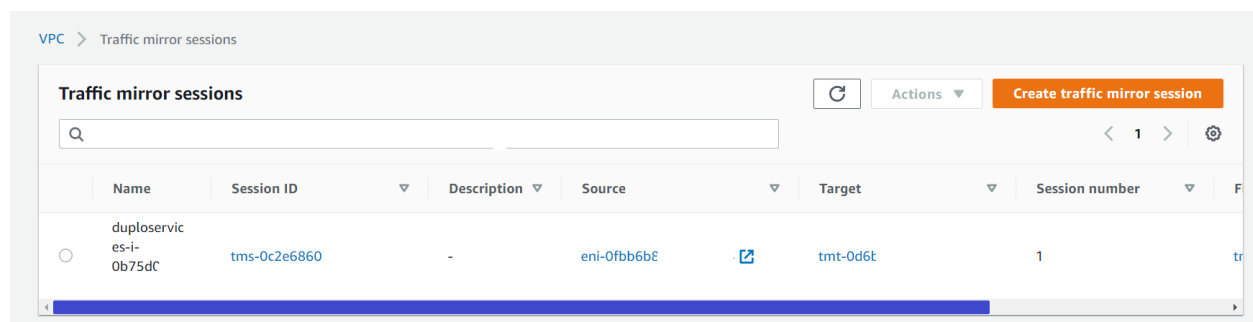
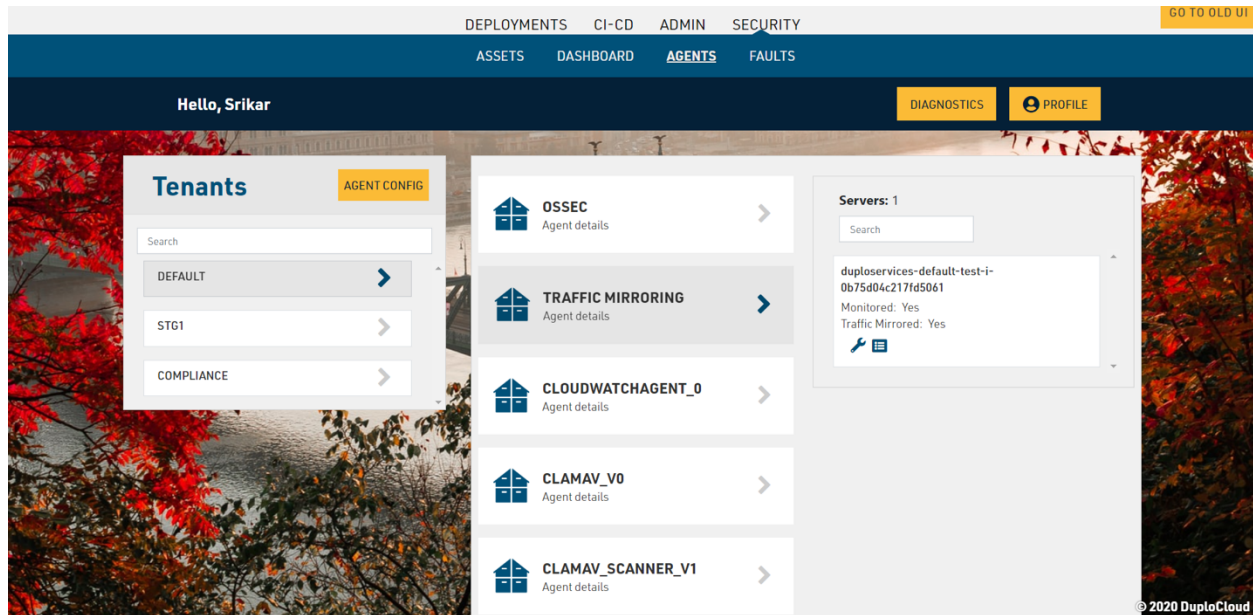
## Virus Scanning (Requirements 5.1, 5.2 & 5.3)

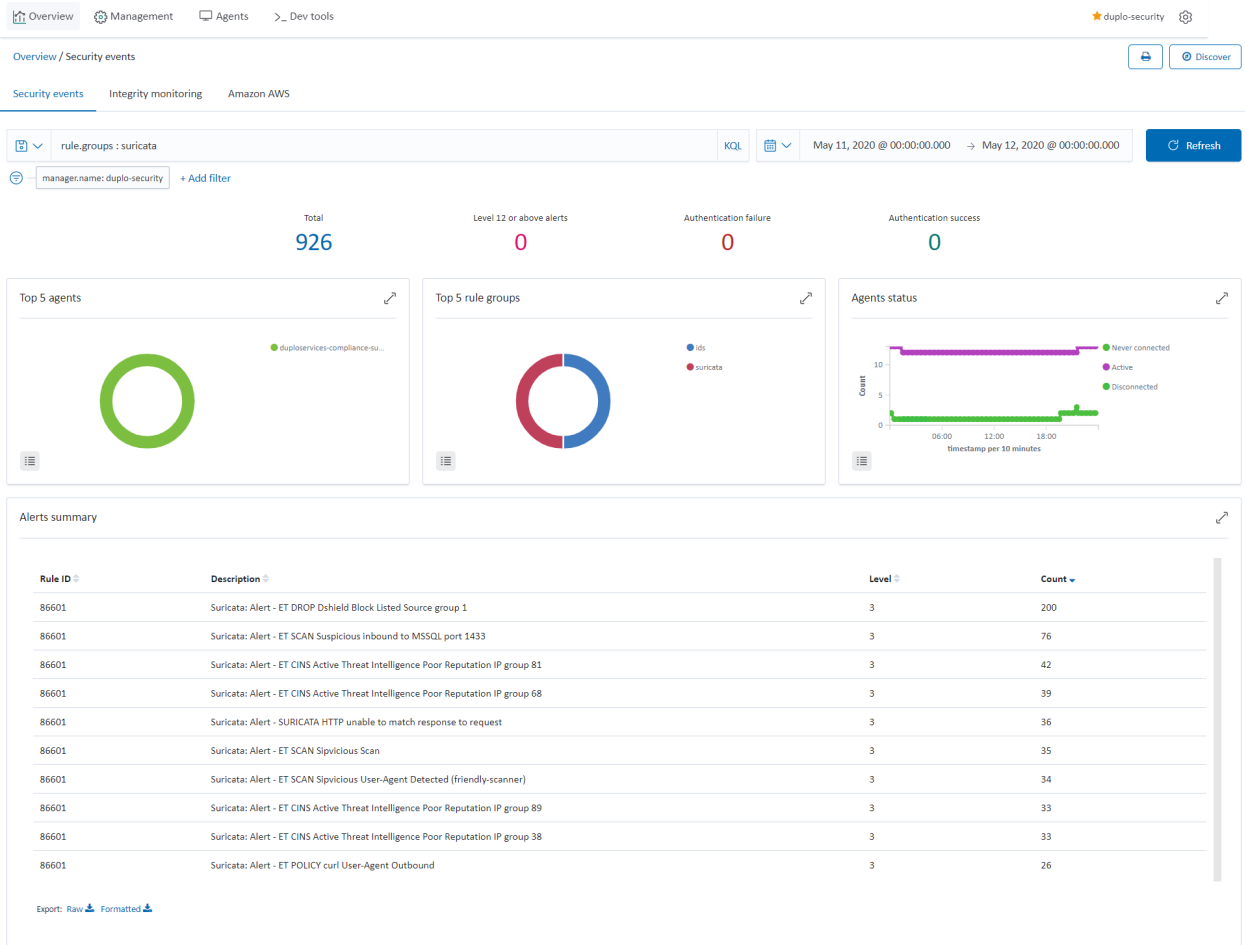
DuploCloud enables ClamAV deployment via agent modules, with alerts collected and categorized in SIEM. Make sure the ClamAV agent module is enabled in DuploCloud. For more information on how to enable this, refer to the config in the “Other Agents” section. DuploCloud will make sure that the ClamAV agent 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 (Requirement 11.4)

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 (Requirement 11)

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](#).

OverviewManagementAgents> Dev tools

Agents / duplocloud-hardware1-host2-i-030c116d6d618a31 (166) / Inventory dataActive

Security eventsIntegrity monitoringInventory data

Cores: 1Memory: 1.991.72 MBArch: x86\_64OS: Amazon Linux 2CPU: Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHzLast scan: 2020/09/20 15:12:30

Network interfaces

Name	MAC	State	MTU	Type
eth1	08:3d:9b:8b:5b:5e	up	9001	ethernet
eth0	08:a6:6d:a2:73:a6	up	9001	ethernet
ens2889d5750	a2:03:b6:cc:72:5e	up	9001	ethernet

Network ports

Local IP	Local port	State	Protocol
::	32760	listening	tcp6
::	63878	listening	tcp6
::	111	listening	tcp6
::	30000	listening	tcp6
::	30256	listening	tcp6
::	30001	listening	tcp6
::	4243	listening	tcp6
::	22	listening	tcp6
127.0.0.1	50051	listening	tcp
127.0.0.1	30248	listening	tcp

Network settings

Interface	Address	Network	Protocol	Broadcast
eth1	10.188.26.56	255.255.240.0	IPv4	10.188.31.255
eth1	fe80::3d:9b:8b:5b:5e	:::::ffff::	IPv6	-
eth0	10.188.25.181	255.255.240.0	IPv4	10.188.31.255
eth0	fe80::a6:6d:a2:73:a6	:::::ffff::	IPv6	-
ens2889d5750	fe80::a2:03:b6:cc:72:5e	:::::ffff::	IPv6	-

Packages

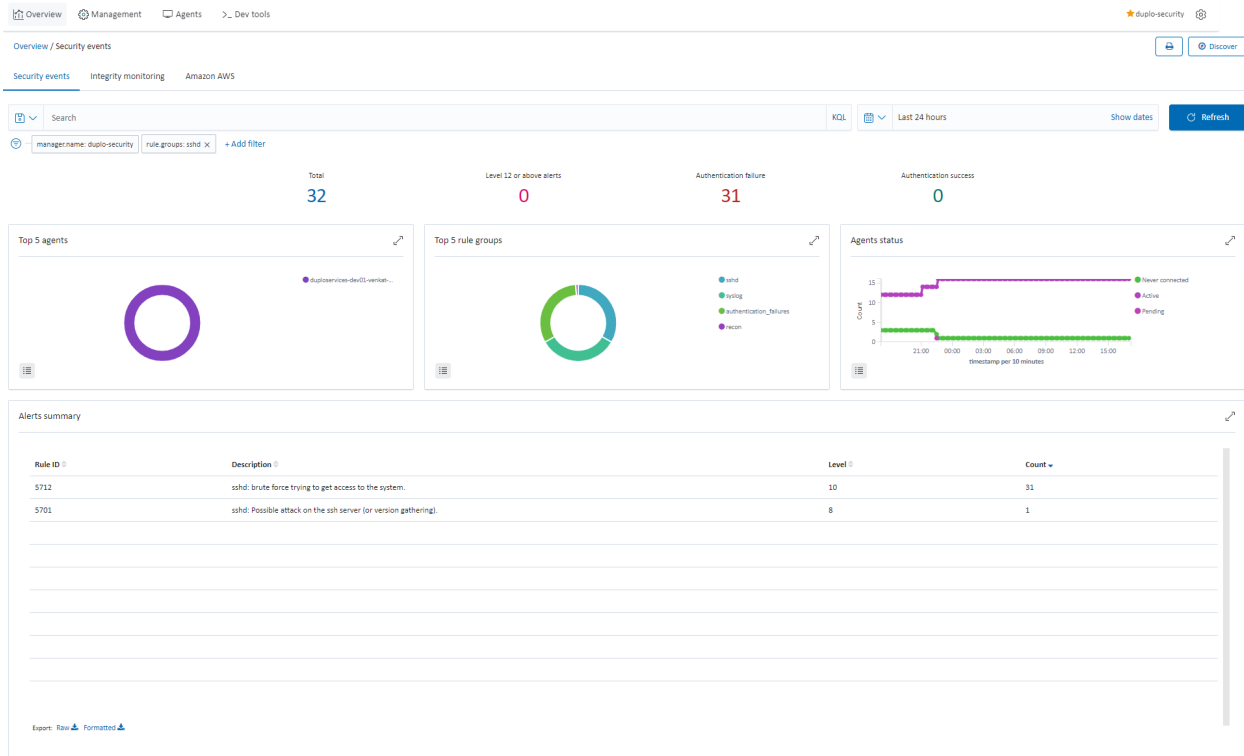
Name	Architecture	Version	Vendor	Description
zlib	x86_64	1.2.7-17.amzn2.0.2	Amazon Linux	The compression and decompression library
yum-utils	noarch	1.1.31-46.amzn2.0.1	Amazon Linux	Utilities based around the yum package manager
yum-plugin-priorities	noarch	1.1.31-46.amzn2.0.1	Amazon Linux	plugin to give priorities to packages from different repos
yum-metadata-parser	x86_64	1.1.4-10.amzn2.0.2	Amazon Linux	A fast metadata parser for yum
yum	noarch	3.4.3-156.amzn2.0.2	Amazon Linux	RPM package installer/updater/manager
xz-libs	x86_64	5.2.2-1.amzn2.0.2	Amazon Linux	Libraries for decoding LZMA compression
xz	x86_64	5.2.2-1.amzn2.0.2	Amazon Linux	LZMA compression utilities
xfsprogs	x86_64	4.5.0-18.amzn2.0.1	Amazon Linux	Utilities for managing the XFS filesystem
which	x86_64	2.20-7.amzn2.0.2	Amazon Linux	Displays where a particular program in your path is located
wget	x86_64	1.14-18.amzn2.1	Amazon Linux	A utility for retrieving files using the HTTP or FTP protocols

Processes

Name	Effective user	Effective group	PID	Parent PID	Command	Args	VM size	Size	Session	Priority	State
systemd	root	root	1	0	/usr/lib/systemd/systemd	--switched-root--system--deserialize=21	125792	33448	1	0	interruptible sleep (waiting for an event to complete)
kthreadd	root	root	2	0	-	-	0	0	0	0	interruptible sleep (waiting for an event to complete)
kworker/0/0	root	root	4	2	-	-	0	0	0	-20	idle
mm_percpu_wq	root	root	6	2	-	-	0	0	0	-20	idle
ksoftirqd/0	root	root	7	2	-	-	0	0	0	0	interruptible sleep (waiting for an event to complete)
rcu_sched	root	root	8	2	-	-	0	0	0	0	idle
rcu_bh	root	root	9	2	-	-	0	0	0	0	idle
migrator/0	root	root	10	2	-	-	0	0	0	0	interruptible sleep (waiting for an event to complete)
watchdog/0	root	root	11	2	-	-	0	0	0	0	interruptible sleep (waiting for an event to complete)
cpuhp/0	root	root	12	2	-	-	0	0	0	0	interruptible sleep (waiting for an event to complete)

## Host Intrusion Detection (Requirement 10.6.1)

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.

[View on Sentry](#)

### New alert from **misp-wazuh-poc**

ISSUE

**Info** **ClamAV: Virus detected - duplo-service...**

May 18, 2020, 2:16:31 p.m. UTC ID: 2ee1b170f4674f69b22ddeab9def0800

#### Message

```
ClamAV: Virus detected - duplo-services-dev01-host2-i-0f204087cfb0ad518- Alert level: 8
```

#### Tags

level = **info**

runtime = **CPython 2.7.12**

runtime.name = **CPython**

server\_name = **duplo-security**

You are receiving this email due to matching rules: [Send a notification for new issues](#)

## 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](#).



## Control-by-Control PCI Implementation Detail

	PCI DSS Requirements v3.2.1	DuploCloud Implementation
1.	1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the Internal network zone	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/ 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.
2.	1.1.5 Description of groups, roles, and responsibilities for management of network components.	DuploCloud overlays logical constructs of Tenant and infrastructure that represents an application. Within a tenant there are concepts of services. All resources within the tenant are by default labeled in the cloud with the Tenant name. Further the automation allows the user to set any tag at a tenant level and that is automatically propagated to AWS/Azure artifacts. The system is always kept in sync with background threads
3.	1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	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/ 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.
4.	1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	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/ Subnet, NSG and Managed Identity in Azure per tenant. By default, no access is

		allowed into the tenant unless specific ports are exposed via ELB.
5.	1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	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/ Subnet, NSG and Managed Identity in Azure per tenant. By default, no access is allowed into the tenant unless specific ports are exposed via ELB.
6.	1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	By default, all outbound traffic uses NAT Gateway. We can put in place additional subnet ACLs if needed. Nodes in the private subnets can only go outside only via a NAT Gateway. In Azure outbound can be blocked in the VNET
7.	1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	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 frontend UI is in a different tenant
8.	1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties.	Use Private subnets and private R53 hosted zones/Private Azure DNS zones
9.	1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties	Usage of a rules-based approach makes the configuration error free, consistent and documented. Further documentation is to be done by the client and we also put in documentation during the blue printing process
10.	2.1 Always change vendor-supplied defaults and remove or disable	DuploCloud enables user specified password or random password generation options. User access is managed in

	<p>unnecessary default accounts before installing a system on the network.</p> <p>This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.)</p>	<p>such a way that all end user access is via single sign on and password less. Even access to AWS/Azure console is done by generating a federated console URL that has a validity of less than an hour. The system enables operations with minimal user accounts as most access is JIT</p>
11.	<p>2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)</p> <p>Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.</p>	<p>DuploCloud orchestrates K8 node selectors for this and supports non container workloads and allows labeling of VMs and achieving this. For non-container workloads are also supported and hence allows automation to meet these controls. For example, one can install Wazuh in one VM, Suricata in another and Elastic Search in another</p>
12.	<p>2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.</p>	<p>By default, no traffic is allowed inside a tenant boundary unless exposed via an LB. DuploCloud allows automated configuration of desired inter-tenant access w/o users needing to manually write scripts. Further as the env changes dynamically DuploCloud keys these configs in sync. DuploCloud also reconciles any orphan resources in the system and cleans them up, this includes docker containers, VMs, LBs, keys, S3 buckets and various other resources</p>
13.	<p>2.2.3 Implement additional security features for any required services, protocols, or daemons that are insecure.</p> <p>Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.</p>	<p>DC gets certificates from Cert-Manager and automates SSL termination in the LB</p>
14.	<p>2.2.4 Configure system security parameters to prevent misuse.</p>	<p>IAM configuration and policies in AWS/ Managed Identities in Azure that implement separation of duties and least</p>

		privilege, S3 bucket policies. 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 frontend UI is in a different tenant
15.	2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	DuploCloud reconciles any orphan resources in the system against the user specifications in its database and cleans them up, this includes docker containers, VMs, LBs, keys, S3 buckets and various other resources. All resources specified by the user in the database are tracked and audited every 30 seconds
16.	2.3 Encrypt all non-console administrative access using strong cryptography.	SSL LB and VPN connections are orchestrated. DuploCloud automates OpenVPN P2S VPN user management by integrating it with user's single sign on i.e., when a user's email is revoked from DuploCloud portal, it is cleaned up automatically from the VPN server
17.	2.4 Maintain an inventory of system components that are in scope for PCI DSS.	All resources are stored in DB, tracked, and audited. The software has an inventory of resources that can be exported
Requirement 3: Protect stored cardholder data		
18.	3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must	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

	<p>not be associated with user accounts.</p> <p>Note: This requirement applies in addition to all other PCI DSS encryption and key-management requirements.</p>	
19.	<p>3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.</p>	<p>DuploCloud orchestrates AWS KMS/Azure Key Vault keys per tenant to encrypt various AWS/Azure resources 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</p>
20.	<p>3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:</p> <ul style="list-style-type: none"> <li>• Encrypted with a key-encrypting key that is at least as strong as the data encrypting key, and that is stored separately from the data-encrypting key</li> <li>• Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device)</li> <li>• As at least two full-length key components or key shares, in accordance with an industry accepted method</li> </ul> <p>Note: It is not required that public keys be stored in one of these forms.</p>	<p>DuploCloud orchestrates AWS KMS/Azure Key Vault for this and that in turns provides this control that we inherit</p>
Requirement 4: Encrypt transmission of cardholder data across open, public networks		
21.	<p>4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:</p>	<p>In the secure infrastructure blueprint we adopt Application Load Balancers with HTTPS listeners. HTTP listeners forwarded to HTTPS. The latest cipher is used in the LB automatically by the DuploCloud software</p>

	<ul style="list-style-type: none"> <li>• Only trusted keys and certificates are accepted.</li> <li>• The protocol in use only supports secure versions or configurations.</li> <li>• The encryption strength is appropriate for the encryption methodology in use.</li> </ul> <p>Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed. Examples of open, public networks include but are not limited to:</p> <ul style="list-style-type: none"> <li>• The Internet</li> <li>• Wireless technologies, including 802.11 and Bluetooth</li> <li>• Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)</li> <li>• General Packet Radio Service (GPRS)</li> <li>• Satellite communications</li> </ul>	
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs		
22.	5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	DuploCloud enables ClamAV deployment via agent modules and alerts are collected in Wazuh
23.	5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	DuploCloud agent modules can be enabled
24.	<p>5.2 Ensure that all anti-virus mechanisms are maintained as follows:</p> <ul style="list-style-type: none"> <li>• Are kept current,</li> <li>• Perform periodic scans</li> </ul>	DuploCloud enables ClamAV deployment via agent modules and alerts are collected in Wazuh.

	<ul style="list-style-type: none"> <li>• Generate audit logs which are retained per PCI DSS Requirement 10.7</li> </ul>	
25	<p>5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.</p> <p>Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.</p>	DuploCloud agent modules do thousand raise an alert if a service is not running
Requirement 6: Develop and maintain secure systems and applications		
26.	<p>6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.</p> <p>Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.</p> <p>Methods for evaluating vulnerabilities and assigning risk</p>	DuploCloud installs by default Wazuh agent and AWS Inspector and any other Agent modules in all VMs and keeps them active. In case any node is failing the auto install DC raises an alarm. In Wazuh the alerts are configured and generated. We rely on the customer's SOC team to act on the alerts. DuploCloud team is the second line of defense if the issue cannot be addressed by client team

	<p>ratings will vary based on an organization's environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.</p>	
27.	<p>6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches. Install critical security patches within one month of release.</p> <p>Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.</p>	Patch management is done as part of DuploCloud SOC offering
28.	<p>6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following:</p> <ul style="list-style-type: none"> <li>• Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices.</li> </ul>	DuploCloud's CI/CD offering provides an out-of-box integration with SonarQube that can be integrated into the pipeline to scan the code.



	<ul style="list-style-type: none"> <li>• Code reviews ensure code is developed according to secure coding guidelines</li> <li>• Appropriate corrections are implemented prior to release.</li> <li>• Code-review results are reviewed and approved by management prior to release</li> </ul> <p>Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.</p>	
Requirement 7: Restrict access to cardholder data by business need to know		
29.	<p>7.1.1 Define access needs for each role, including:</p> <ul style="list-style-type: none"> <li>• System components and data resources that each role needs to access for their job function</li> <li>• Level of privilege required (for example, user, administrator, etc.) for accessing resources</li> </ul>	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 in AWS/NSG in Azure. Tenant access policies will automatically apply SG or IAM based policy in AWS/NSG, or Managed Identity in Azure based on the resource type.
	<p>7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed. This access control system(s) must include the following</p>	User access to AWS/Azure console is granted based on tenant permissions and least privilege and a Just in time federated token that expires in less than an hour. Admins have privileged access and read-only user is another role
30.	<p>7.2.1 Coverage of all system components.</p>	AWS resource access is controlled based on IAM role, SG and static VPN client Ips/ Azure resource access in

		controlled by NSG, Managed Identity and static VPN client Ips that are all implicitly orchestrated and kept up to date
31.	7.2.3 Default deny-all setting.	This is the default DuploCloud implementation of Sg and IAM roles in AWS/NSG and Managed Identity in Azure
Requirement 8: Identify and authenticate access to system components		
32.	8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal. From there a federated logic is done for AWS/Azure resource access
33.	8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	This is done at infra level in DuploCloud portal using single sign on
34.	8.1.3 Immediately revoke access for any terminated users.	DuploCloud integrates with client's IDP like G Suite 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
35.	8.1.4 Remove/disable inactive user accounts within 90 days.	DuploCloud integrates with client's IDP like G Suite 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
36.	8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: <ul style="list-style-type: none"> <li>• Enabled only during the time period needed and disabled when not in use.</li> <li>• Monitored when in use.</li> </ul>	DuploCloud integrates by calling STS API to provide JIT token and URL
37.	8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal. When DuploCloud managed OpenVPN is used it is setup to lock the user out after failed attempts

38.	8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal. When DuploCloud managed OpenVPN is used it is setup to lock the user out after failed attempts. In Open VPN an admin must unlock the user
39.	8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	DuploCloud single sign on has configurable timeout. For AWS/Azure resource access we provide JIT access
40.	8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: <ul style="list-style-type: none"> <li>• Something you know, such as a password or passphrase</li> <li>• Something you have, such as a token device or smart card</li> <li>• Something you are, such as a biometric.</li> </ul>	DuploCloud relies on the client's single sign on / IDP. If the user secures his corporate login using these controls, then by virtue of single sign on, this gets implemented in the infrastructure.
41.	8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	Encryption at REST is done via AWS KMS/Azure KeyVault and in transit via SSL
42.	8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal.
43.	8.2.3 Passwords/phrases must meet the following: <ul style="list-style-type: none"> <li>• Require a minimum length of at least seven characters.</li> <li>• Contain both numeric and alphabetic characters.</li> </ul> Alternatively, the passwords/phrases must have	Enforced by AWS/Azure and should be enforced by client's IDP. DuploCloud integrates with the IDP. The control should be implemented by the organization IDP.

	complexity and strength at least equivalent to the parameters specified above.	
44.	8.2.4 Change user passwords/passphrases at least every 90 days.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal.
45.	8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	Enforced by AWS/Azure and should be enforced by client's IDP. DuploCloud integrates with the IDP. The control should be implemented by the organization IDP.
46.	8.2.6 Set passwords/phrases for first time use and upon reset to a unique value for each user and change immediately after the first use.	Enforced by AWS/Azure and should be enforced by client's IDP. DuploCloud integrates with the IDP. The control should be implemented by the organization IDP,
47.	8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. Note: Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal. Open VPN has MFA enabled
48.	8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal. Open VPN has MFA enabled
49.	8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator and including third-party access for support or	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal. Open VPN has MFA enabled

	maintenance) originating from outside the entity's network.	
50.	<p>8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:</p> <ul style="list-style-type: none"> <li>• All user access to, user queries of, and user actions on databases are through programmatic methods.</li> <li>• Only database administrators have the ability to directly access or query databases.</li> <li>• Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes)</li> </ul>	The IAM integration with the database makes SQL connections also via Instance Profile. For users, individual JIT access is granted that lasts only 15 mins
Requirement 10: Track and monitor all access to network resources and cardholder data		
51.	10.1 Implement audit trails to link all access to system components to each individual user.	DuploCloud maintains trails in 2 places in addition to cloud trails. It logs all write events about infrastructure change in an ELK cluster. Further Wazuh agent tracks all activities at the host level. All 3 - Cloud trail, audit and Wazuh agent events are brought together in the Wazuh dashboard
52.	10.2.1 All individual user accesses to cardholder data.	Infrastructure updates are audited and stored in ELK. Access to DB is through JIT access. SSH access to VMs are done via Wazuh syslog collection
52.	10.2.2 All actions taken by any individual with root or administrative privileges.	Infrastructure updates are audited and stored in ELK. Access to DB is through JIT access. SSH access to VMs are done via Wazuh syslog collection
53.	10.2.3 Access to all audit trails.	Infrastructure updates are audited and stored in ELK. Access to DB is through JIT access. SSH access to VMs are done via Wazuh syslog collection
54.	10.2.4 Invalid logical access attempts.	Cloud trails and syslog hold this information which is stored in the centralized SIEM (Wazuh)
55.	10.2 5 Use of and changes to identification and authentication mechanisms—including but not	Infrastructure updates are audited and stored in ELK. Access to DB is through JIT access. SSH access to VMs are done via Wazuh syslog collection

	limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.	
56.	10.2.6 Initialization, stopping, or pausing of the audit logs	AWS IAM policies prevent start/stop of AWS CloudTrail, S3 bucket policies protect access to log data, alerts are sent if AWS CloudTrail is disabled, AWS Config rule provides monitoring of AWS CloudTrail enabled
57.	10.2.7 Creation and deletion of system level objects	DuploCloud maintains trails in 2 places in addition to cloud trail. It logs all write events about infrastructure change in an ELK cluster. Further, Wazuh agent tracks all activities at the host level. All 3 - Cloud trail, audit and Wazuh agent events are brought together in the Wazuh dashboard
	10.3 Record at least the following audit trail entries for all system components for each event:	
58	10.3.1 User identification.	DuploCloud maintains trails in 2 places in addition to cloud trail. It logs all write events about infrastructure change in an ELK cluster. Further, Wazuh agent tracks all activities at the host level. All 3 - Cloud trail, audit and Wazuh agent events are brought together in the Wazuh dashboard
59.	10.3.2 Type of event.	DuploCloud maintains trails in 2 places in addition to cloud trail. It logs all write events about infrastructure change in an ELK cluster. Further, Wazuh agent tracks all activities at the host level. All 3 - Cloud trail, audit and Wazuh agent events are brought together in the Wazuh dashboard
60.	10.3.3 Date and time.	DuploCloud maintains trails in 2 places in addition to cloud trail. It logs all write events about infrastructure change in an ELK cluster. Further, Wazuh agent tracks all activities at the host level. All 3 - Cloud trail, audit and Wazuh agent events are brought together in the Wazuh dashboard
61.	10.3.4 Success or failure indication.	DuploCloud maintains trails in 2 places in addition to cloud trail. It logs all write events about infrastructure change in an ELK cluster. Further, Wazuh agent tracks all activities at the host level. All 3 - Cloud trail, audit and Wazuh agent events are brought together in the Wazuh dashboard
62.	10.3.5 Origination of event.	DuploCloud maintains trails in 2 places in addition to cloud trail. It logs all write events about infrastructure change in an ELK cluster. Further, Wazuh agent tracks all activities at

		the host level. All 3 - Cloud trail, audit and Wazuh agent events are brought together in the Wazuh dashboard
63.	10.3.6 Identity or name of affected data, system component, or resource.	DuploCloud maintains trails in 2 places in addition to cloud trail. It logs all write events about infrastructure change in an ELK cluster. Further, Wazuh agent tracks all activities at the host level. All 3 - Cloud trail, audit and Wazuh agent events are brought together in the Wazuh dashboard
64.	10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).	All instances launched in VPC are synced with NTP. User data is injected for time sync
65.	10.4.1 Critical systems have the correct and consistent time.	All instances launched in VPC are synced with NTP using user data that is implicitly added. All log data has timestamp provided by NTP
66.	10.4.3 Time settings are received from industry-accepted time sources.	All instances launched in VPC are synced with AWS NTP servers which in turn obtain time from NTP.org
67.	10.5.1 Limit viewing of audit trails to those with a job-related need.	Audit trails views access are part of the DuploCloud Access controls
68.	10.5.2 Protect audit trail files from unauthorized modifications.	Cloud trails policies are set in place. Wazuh and ELK access is limited to admins
69.	10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	This is done automatically by DuploCloud
70.	10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	DuploCloud maintains trails in 2 places in addition to cloud trail. It logs all write events about infrastructure change in an ELK cluster. Further, Wazuh agent tracks all activities at the host level. All 3 - Cloud trail, audit and Wazuh agent events are brought together in the Wazuh dashboard
71.	10.5.5 Use file integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without	We stored Cloud trail data in a separate AWS account. Wazuh has FIM

	generating alerts (although new data being added should not cause an alert).	
72.	<p>10.6.1 Review the following at least daily:</p> <ul style="list-style-type: none"> <li>• All security events</li> <li>• Logs of all system components that store, process, or transmit CHD and/or SAD</li> <li>• Logs of all critical system components</li> <li>• Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).</li> </ul>	Done by DuploCloud SOC Team
73.	10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	DuploCloud automatically snapshots the SIEM after the indexes grow beyond a certain size (minimum 3 months) and deletes the index in the running system. Any old index can be brought back in a few clicks. The indexes are per day which makes it straight forward to meet compliance guidelines like 3 months in this case
Requirement 11: Regularly test security systems and processes		
74.	<p>11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).</p> <p>Note: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated</p>	Offered as part of DuploCloud SOC



	<p>vulnerabilities are in the process of being addressed.</p> <p>For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s).</p> <p>For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.</p>	
75.	<p>11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all “high risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.</p>	Offered as part of DuploCloud SOC
76.	<p>11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.</p>	DuploCloud enables WAF rules to mitigate many of these vulnerabilities if the application change is less viable
77.	<p>11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network.</p> <p>Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.</p>	<p>DuploCloud orchestrates AWS Traffic mirroring to send a copy of the traffic at all critical points (tenants) to a Suricata VM. From there the alerts are fetched by Wazuh and displayed in the central dashboard. This provides IDS but if prevention is desired then the Suricata software is enabled in each critical VM preferably in the AMI (Image) itself. The alerts are then fetched by the Wazuh agent and updated in Wazuh SIEM</p>

78.	<p>11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.</p> <p>Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come preconfigured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider)</p>	DuploCloud orchestrates installation and update of Wazuh agent is all servers that are launched. Wazuh agent then performs FIM and raises alerts. The alerts will first be triaged by the client SOC team
79.	11.5.1 Implement a process to respond to any alerts generated by the change detection solution.	DuploCloud SOC team will receive the email and operate as per the defined and approved Incident management solution

## Control-by-Control HIPAA Implementation Detail

	HIPAA Regulation Text	DuploCloud Implementation
1.	<p>§164.306(a) Covered entities and business associates must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or</p>	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.

	hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part; and (4) Ensure compliance with this subpart by its workforce.	
2.	§164.308(a) A covered entity or business associate must in accordance with §164.306: (1)(i) Implement policies and procedures to prevent, detect, contain, and correct security violations.	Usage of a rules-based approach makes the configuration error free, consistent, and documented. In addition, DuploCloud also provides audit trails for any change in the system.
3.	§164.308(a)(1)(ii)(A) Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	Inherited from AWS.
4.	§164.308(a)(1)(ii)(B) Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).	Usage of a rules-based approach makes the configuration error free, consistent, and documented. Further documentation is to be done by the client and we also put in documentation during the blue printing process.
5.	§164.308(a)(1)(ii)(D) Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	DuploCloud maintains trails in 2 places in addition to cloud trail. It logs all write events about infrastructure change in an ELK cluster. Further, Wazuh agent tracks all activities at the host level. All 3 - Cloud trail, audit and Wazuh agent events are brought together in the Wazuh dashboard.
6.	§164.308(a)(3)(i) Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those	DuploCloud automation introduces a concept of a tenant which is a logical construct above AWS and represents an application's entire lifecycle. It is a security boundary implemented by having a unique SG, IAM Role and Instance Profile per tenant. By default, no access is allowed into the tenant unless specific ports are exposed via ELB.

	workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	
7.	§164.308(a)(5)(ii)(C) Procedures for monitoring log-in attempts and reporting discrepancies.	DuploCloud maintains trails in 2 places in addition to cloud trail. It logs all write events about infrastructure change in an ELK cluster. Further, Wazuh agent tracks all activities at the host level. All 3 - Cloud trail, audit and Wazuh agent events are brought together in the Wazuh dashboard.
8.	§164.308(a)(5)(ii)(D) Procedures for creating, changing, and safeguarding passwords.	DuploCloud enables user specified password or random password generation options. User access is managed in such a way that all end user access is via single sign on and password less. Even access to AWS console is done by generating a federated console URL that has a validity of less than an hour. The system enables operations with minimal user accounts as most access is JIT.
9.	§164.308(a)(6)(i) Implement policies and procedures to address security incidents.	Duplo orchestrates with Wazuh as SIEM. Wazuh agents are automatically installed in the hosts and is integrated with various services like CloudWatch, cloud trail, inspector and Suricata. Which collects the vulnerabilities, and all of those vulnerabilities can be view in one page.
10.	§164.308(a)(6)(ii) Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	Duplo orchestrates with Wazuh as SIEM. Wazuh agents are automatically installed in the hosts and is integrated with various services like CloudWatch, cloud trail, inspector and Suricata. Which collects the vulnerabilities, and all of those vulnerabilities can be view in one page.
11.	§164.308(a)(7)(i) Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (As one illustrative example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	Duplo infrastructure is created with 2 or more availability zones. With this alternate storage and processing capability that dynamically provides transfer and resumption of system operation in times of failure.

12.	§164.308(a)(7)(ii)(A) Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	Inherited from AWS.
13.	§164.308(a)(7)(ii)(B) Establish (and implement as needed) procedures to restore any loss of data.	DuploCloud automation includes DR and BCP. This includes data backups for services like S3, EBS and RDS. The automation supports multi-regions with the platform that can be deployed in different regions as per the BCP needs. The MTTR is minimized and is typically less than an hour by virtue of the automation.
14.	§164.308(a)(7)(ii)(C) Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	Duplo infrastructure is created with 2 or more availability zones. With this alternate storage and processing capability that dynamically provides transfer and resumption of system operation in times of failure.
15.	§164.310(a)(2)(i) Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	Duplo infrastructure is created with 2 or more availability zones. With this alternate storage and processing capability that dynamically provides transfer and resumption of system operation in times of failure.
16.	§164.310(a)(2)(iii) Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	DuploCloud's single sign on functionality over various cloud system accesses enable a Just in time and secure access to software systems. DuploCloud enables user specified password or random password generation options. User access is managed in such a way that all end user access is via single sign on and password less. Even access to AWS console is done by generating a federated console URL that has a validity of less than an hour. Multiple other systems like SIEM, Elastic search dashboards for Auditor, Log viewing etc are also integrated into the single sign on.
17.	§164.310(d)(2)(iv) Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	Inherited from AWS.

18.	§164.312(a)(1) Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).	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.
19.	§164.312(a)(2)(i) Assign a unique name and/or number for identifying and tracking user identity.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal. From there a federated logic is done for AWS resource access.
20.	§164.312(a)(2)(ii) Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	Duplo infrastructure is created with 2 or more availability zones. With this alternate storage and processing capability that dynamically provides transfer and resumption of system operation in times of failure.
21.	§164.312(a)(2)(iii) Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Inherited from AWS.
22.	§164.312(a)(2)(iv) Implement a mechanism to encrypt and decrypt electronic protected health information.	DuploCloud orchestrates KMS keys per tenant to encrypt various AWS resource in that tenant like RDS DBs, S3, Elastic Search, REDIS etc. Access to the KMS keys is granted only to the instance profile w/o any user accounts or keys. By default, DuploCloud creates a common KMS key per deployment but allows ability to have one key per tenant.
23.	§164.312(b) Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	DuploCloud maintains trails in 2 places in addition to cloud trail. It logs all write events about infrastructure change in an ELK cluster. Further, Wazuh agent tracks all activities at the host level. All 3 - Cloud trail, audit and Wazuh agent events are brought together in the Wazuh dashboard.
24.	§164.312(c)(1) Implement policies and procedures to protect electronic protected health	DuploCloud automation introduces a concept of a tenant which is a logical construct above AWS and represents an application's entire lifecycle. It is a security boundary implemented by having a unique SG, IAM Role and

	information from improper alteration or destruction.	Instance Profile per tenant. By default, no access is allowed into the tenant unless specific ports are exposed via ELB.
25.	§164.312(c)(2) Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	DuploCloud automation introduces a concept of a tenant which is a logical construct above AWS and represents an application's entire lifecycle. It is a security boundary implemented by having a unique SG, IAM Role and Instance Profile per tenant. By default, no access is allowed into the tenant unless specific ports are exposed via ELB.
26.	§164.312(e)(1) Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	DC gets certificates from Cert-Manager and automates SSL termination in the ELB. In addition, TLS/SSH ports are enforced in the security groups by the DuploCloud.
27.	§164.312(e)(2)(i) Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	DuploCloud by default orchestrates appropriate services like Encryption at rest and transit to protect data integrity.
28.	§164.312(e)(2)(ii) Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	DuploCloud orchestrates KMS keys per tenant to encrypt various AWS resource in that tenant like RDS DBs, S3, Elastic Search, REDIS etc. Access to the KMS keys is granted only to the instance profile w/o any user accounts or keys. By default, DuploCloud creates a common KMS key per deployment but allows ability to have one key per tenant.

## Control-by-Control HITRUST Implementation Detail

	HITRUST CSF Requirement Statement	DuploCloud Implementation
	02 Endpoint Protection	

1	0265.09m1Organizational.2 - The organization applies a default-deny rule that drops all traffic via host-based firewalls or port filtering tools on its endpoints (workstations, servers, etc.), except those services and ports that are explicitly allowed.	All cloud based infrastructure comes with a default deny rule at the Cloud Service Provider security group level.
03 Portable Media Security		
2	0304.09o1Organizational.2 - The organization restricts the use of writable, removable media and personally owned, removable media in organizational systems.	For cloud infrastructure this is inherited from the Cloud Service Provider
06 Configuration Management		
3	06.09b1System.2 - Changes to information systems (including changes to applications, databases, configurations, network devices, and operating systems and with the potential exception of automated security patches) are consistently documented, tested, and approved.	All changes go through a change management process, which includes: tickets, peer reviewed, testing in non production environments, and only applied to production when all required approvals have been met.
4	0613.06h1Organizational.12 - The organization performs annual checks on the technical security configuration of systems, either manually by an individual with experience with the systems and/or with the assistance of automated software tools. If any non-compliance is found as a result of a technical security configuration compliance review, the organization: determines the causes of the non-compliance; evaluates the need for actions to ensure that non-compliance do not recur;	SAST based scanning is integrated into the CI process and DAST based scanning is performed on a frequent basis.



	determines and implements appropriate corrective action; and reviews the corrective action taken.	
5	<p>0627.10h1System.45 - Vendor supplied software used in operational systems is maintained at a level supported by the supplier and uses the latest version of Web browsers on operational systems to take advantage of the latest security functions.</p> <p>The organization maintains information systems according to a current baseline configuration and configures system security parameters to prevent misuse.</p>	With the asset inventory that DuploCloud maintains a periodic review of the inventory is performed to ensure all vendor supplied software versions are maintained
6	<p>0605.10h2System.7 - The updating of operational software, applications, and program libraries is performed by authorized administrators.</p> <p>Operational systems only hold approved programs or executable code (i.e., no development code or compilers). Any decision to upgrade to a new release takes into account the business requirements for the change, the security impacts of the release (e.g., the introduction of new security functionality or the number and severity of security problems affecting this version), and privacy impacts of the release.</p>	Access to pipelines that updates production environments is limited to a subset of users who need access.
7	<p>0606.10h2System.1 - The organization ensures applications and operating system software are only implemented after successful testing.</p> <p>Pre-implementation tests: include tests on usability;</p>	All changes go through a change management process, which includes: tickets, peer reviewed, testing in non production environments, and only applied to production when all required approvals have been met.

	include tests on security; include tests on effects on other systems; and are carried out on separate systems.	
8	0663.10h2System.9 - The operating system is required to have in place supporting technical controls such as antivirus, file integrity monitoring, host-based (personal) firewalls or port filtering tools, and logging as part of their baseline.	DuploCloud enables ClamAV, file integrity monitoring, and log collection via agent modules and alerts are collected in Wazuh. Host based firewall rules are implemented at the Cloud Service Provider level.
	07 Vulnerability Management	
9	07.07a1Organizational.8 - Organizational inventories of IT assets are periodically (annually at minimum) reviewed to ensure completeness and accuracy.	All resources are stored in DB, tracked, and audited. The software has an inventory of resources that can be exported for review on an annual basis.
10	07.10m1Organizational.2 - The organization deploys automated software update tools in order to ensure that systems are running the most recent security updates provided by the software vendor, and installs software updates manually for systems that do not support automated software updates.	With the use of the SIEM baked into DuploCloud, hosts with updates can easily be identified and updates can be deployed.
11	07.10m1Organizational.3 - Information systems are periodically scanned to proactively (annually at minimum) identify technical vulnerabilities.	DuploCloud installs by default Wazuh agent and AWS Inspector and any other Agent modules in all VMs and keeps them active. In case any node is failing the auto install DC raises an alarm. In Wazuh the alerts are configured and generated. We rely on customer's SOC team to act on the alerts. DuploCloud team is the second line of defense if the issue cannot be addressed by client team
12	0706.10b1System.2 - The organization develops applications based on secure coding guidelines to prevent: common coding vulnerabilities in software development processes; injection flaws, particularly SQL injection (Validate input to verify	Pipelines are enhanced to include SAST and DAST phases to prevent common coding vulnerabilities making their way into production.

	<p>user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.);  buffer overflow (Validate buffer boundaries and truncate input strings);  insecure cryptographic storage (Prevent cryptographic flaws);  insecure communications (Properly encrypt all authenticated and sensitive communications);  improper error handling (Do not leak information via error messages);  broken authentication/sessions (Prevent unauthorized individuals from compromising legitimate account credentials, keys or session tokens that would otherwise enable an intruder to assume the identity of an authorized user);  cross-site scripting (XSS), e.g., validate all parameters before inclusion, utilize context-sensitive escaping, etc.);  improper access control, such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access functions (e.g., properly authenticate users and sanitize input, and do not expose internal object references to users);  cross-site request forgery (CSRF), e.g., do not rely on authorization credentials and tokens automatically submitted by browsers; and  any other input-validation vulnerability listed in the OWASP Top 10.</p>	
13	<p>0707.10b2System.1 - Applications which store, process or transmit covered information undergo automated (non-manual) application vulnerability testing with an emphasis on input validation controls at least annually by a qualified party.</p>	Offered as part of DuploCloud SOC

	08 Network Protection	
14	<p>0825.09m1Organizational.14 - Technical tools such as intrusion detection systems (IDS)/intrusion prevention systems (IPS) are implemented and operating at the network perimeter and key points within the network. Implemented and operating technical tools include IDS and IPDS deployed on the wireless side of the firewall (WIDS). The IDS/IPS is updated on a regular basis, including the engines, baselines and signatures.</p>	<p>DuploCloud orchestrates AWS Traffic mirroring to send a copy of the traffic at all critical points (tenants) to a Suricata VM. From there the alerts are fetched by Wazuh and displayed in the central dashboard. This provides IDS but if prevention is desired then the Suricata software is enabled in each critical VM preferably in the AMI (Image) itself. The alerts are then fetched by the Wazuh agent and updated in Wazuh SIEM</p>
	09 Transmission Protection	
15	<p>0913.09s1Organizational.5 - Formal procedures are defined to encrypt data in transit including use of strong cryptography protocols to safeguard covered and/or confidential information during transmission over less trusted/open public networks. Valid encryption processes include: Transport Layer Security (TLS) 1.2 or later; IPSec VPNs: Gateway-To-Gateway Architecture; Host-To-Gateway Architecture; Host-To-Host Architecture; and TSL VPNs: SSL Portal VPN; SSL Tunnel VPN.</p>	<p>DuploCloud gets TLS certificates from the Cloud Service Provider and automates SSL termination in the LB</p>
16	<p>0936.09w1Organizational.1 - A security baseline is documented and implemented for interconnected systems.</p>	<p>DuploCloud provides a document that details the security baseline of all infrastructure that DuploCloud provisions.</p>
	10 Password Management	
17	<p>1003.01d1System.3 - User identities</p>	<p>DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal.</p>

	are verified prior to performing password resets.	
18	1009.01d2System.4 - Temporary passwords are unique to an individual and are not guessable.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal.
19	1014.01d2System.9 - The organization avoids the use of third-parties or unprotected (clear text) electronic mail messages for the dissemination of passwords.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal.
20	1015.01d2System.10 - Users acknowledge receipt of passwords.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the portal.
	11 Access Control	
21	11.01q1System.3 - The organization requires multi-factor authentication for network and local access to privileged accounts.	DuploCloud integrates with client's IDP like G Suite and O365 for multi-factor authentication. For remote network access OpenVPN has MFA enabled
22	11.01q1System.4 - The organization requires multi-factor authentication for access to non-privileged accounts from remote networks (including accounts in Web applications and in remote access solutions such as VPNs).	DuploCloud integrates with client's IDP like G Suite and O365 for multi-factor authentication. For remote network access OpenVPN has MFA enabled
23	1194.01l1Organizational.2 - Ports, services, and applications installed on a computer or network systems, which are not specifically required for business functionality, are disabled or removed.	Host images are built from automation which acts as a BOM of what is included in all images. Ports and services are only added on an as needed basis.
24	1111.01b2System.1 - User account administration processes do not use group,	There are three levels of access involved: the DuploCloud platform, the Cloud Service Provider, and host level access. Access to the DuploCloud platform is handled via SSO. Access to the Cloud Service Provider and host is

	shared, or generic accounts and passwords.	provided via JIT. Group, shared, or generic service accounts are never used.
25	11112.01q2System.12 - The information system uses replay-resistant authentication mechanisms such as one-time passwords, or time stamps (e.g., Kerberos, TLS, etc.), nonce (a value used in security protocols that is never repeated with the same key) for network access to privileged accounts.	DuploCloud integrates with client's IDP like G Suite and O365 for access to the DuploCloud portal. The IDP can be configured to require MFA.
26	11126.01t2System.2 - The time-out system conceals information previously visible on the display with a publicly viewable image (e.g., a screen saver), pauses the session screen after 15 minutes of inactivity, closes network sessions after 30 minutes of inactivity, and requires the user to reestablish access using appropriate identification and authentication procedures.	DuploCloud single sign on has configurable timeout. For AWS/Azure resource access we provide JIT access
27	1124.01q2System.12 - Shared user/group IDs are only used in exceptional circumstances, where there is a clear business benefit for the use of a shared user ID for a group of users or a specific job. Approval by management is documented when shared user/group IDs are used. Additional controls are required to maintain accountability when shared user/group IDs are used. Generic IDs that are used by an individual are allowed only where the functions accessible or actions carried out by the ID do not need to be traced (e.g., read only access).	With the JIT access capability provided by DuploCloud shared user/group IDs are not required.

28	1125.01q2System.1 - Appropriate authentication methods, including strong authentication methods in addition to passwords, are used for communicating through an external, non-organization-controlled network (e.g., the Internet).	DuploCloud comes bundled with OpenVPN to secure all communication when non-organizational-controlled network usage is required.
29	1145.01c2System.1 - Role-based access controls are implemented and capable of mapping each user to one or more roles, and each role to one or more system functions.	Users within DuploCloud can be assigned a role for a Tenant. Multiple users can be assigned to the same Tenant and a user can be assigned to multiple Tenants.
30	1146.01c2System.23 - The development and use of system routines and programs which avoid the need to run elevated privileges is promoted.	By leveraging the capabilities in DuploCloud avoids the need for common elevated privileges scenarios.
31	1150.01c2System.10 - The access control system for the system components storing, processing, or transmitting covered information is set with a default "deny-all" setting.	By default users in DuploCloud have access to no Tenants until explicitly granted access to a Tenant.
32	11113.01q3System.3 - The organization employs multifactor authentication for remote network access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access. The organization employs multifactor authentication for local access to privileged accounts (including those used for non-local maintenance and diagnostic sessions).	OpenVPN has MFA enabled
33	11180.01c3System.6 - Access to management functions or administrative consoles for systems hosting virtualized systems is restricted to personnel based upon the principle of least privilege and	DuploCloud integrates with client's IDP like G Suite and O365 for access to the DuploCloud portal. The IDP can be configured to require MFA. Additionally the DuploCloud portal can be put behind a VPN and/or network whitelist.

	supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	
	12 Audit Logging & Monitoring	
34	1203.09aa1System.2 - Audit records include a unique user ID, unique data subject ID (if applicable), function performed, and date/time the event was performed.	DuploCloud, the platform, produces an audit trail of every action taken in the system. Additionally, all hosts created by DuploCloud will have auditing enabled at the operating system level.
35	1223.09ac1System.1 - Access to audit trails / logs is safeguarded from unauthorized access and use.	Access to all audit logs is restricted to users with administrative level permissions
36	1235.06j1Organizational.1 - Access to information systems audit tools is protected to prevent any possible misuse or compromise.	DuploCloud RBAC protects access to audit systems.
37	1239.09aa1System.4 - Retention policies for audit logs are specified by the organization and the audit logs are retained accordingly.	DuploCloud manages the retention policy for all audit logs and allows organization to specify durations for the policy.
38	1202.09aa2System.5 - A secure audit record is created each time a user accesses, creates, updates, or deletes covered and/or confidential information via the system.	DuploCloud will ensure configuration is applied that will create an audit trail when covered and/or confidential information via infrastructure related mechanisms (examples: S3, shell access to server, etc). Customer application logic will be required to produce audit trails for data access via the application.
39	1204.09aa2System.6 - The activities of privileged users (administrators, operators, etc.) include the success/failure of the event, time the event occurred, information about the event (e.g., files handled) or failure (e.g., error	DuploCloud, the platform, produces an audit trail of every action taken in the system. Additionally, all hosts created by DuploCloud will have auditing enabled at the operating system level.



	<p>occurred and corrective action taken), the account or administrator involved, and which processes were involved.</p>	
40	<p>1205.09aa2System.1 - Logs of messages sent and received are maintained, such a log contains the time, date, origin, and destination of the message, but not its content.</p>	<p>DuploCloud manages and enforces centralized logging for both hosts and containers.</p>
41	<p>1206.09aa2System.23 - Auditing is always available while the system is active. Audit logs are maintained for: dates, times, and details of key events (e.g., log-on and log-off); records of successful and rejected system access attempts; records of successful and rejected data and other resource access attempts; changes to system configuration and procedures for managing configuration changes; use of privileges; use of system utilities and applications; files accessed and the kind of access; network addresses and protocols; alarms raised by the access control system; activation and de-activation of protection systems, including anti-virus systems and intrusion detection systems, and identification and authentication mechanisms; and creation and deletion of system level objects.</p>	<p>DuploCloud, the platform, produces an audit trail of every action taken in the system. Additionally, all hosts created by DuploCloud will have auditing enabled at the operating system level.</p>
42	<p>1207.09aa2System.4 - The organization ensures audit records are retained for 90 days and old records archived for one year to provide support for after-the-fact investigations of security incidents and to meet regulatory</p>	<p>DuploCloud manages the retention policy for all audit logs and allows organization to specify durations for the policy.</p>

	and the organization's retention requirements.	
43	12100.09ab2System.15 - The organization monitors the information system to identify irregularities or anomalies that are indicators of a system malfunction or compromise and help confirm the system is functioning in an optimal, resilient, and secure state.	DuploCloud automatically centralizes all audit logs into the built in SIEM for analysis
44	1212.09ab2System.5 - The organization complies with all relevant legal requirements applicable to its monitoring of authorized access and unauthorized access attempts.	DuploCloud will document a step by step procedure for reviewing authorized and unauthorized access attempts and schedule reminders for the customer SOC team to perform the review
45	1213.09ab2System.6 - Information systems containing covered and/or confidential information are provided with automated tools for monitoring system events, detecting attacks and analyzing logs and audit trails to support the identification of access to and modification of covered and/or confidential records by a given user over a given period of time. Monitoring devices are deployed at strategic and ad hoc locations to track specific transactions and the impact of security changes to information systems. The organization reviews physical access logs weekly and upon occurrence of security incidents involving physical security. The organization deploys NetFlow-style collection and analysis to DMZ network flows to detect anomalous activity.	DuploCloud comes out of the box with a built in SIEM
46	1214.09ab2System.3456 - Monitoring of privileged operations includes	DuploCloud comes out of the box with a built in SIEM

	<p>the use of privileged accounts, system start-up and stop, and I/O device attachment/detachment. Monitoring of authorized access includes the user ID, date and time of key events, types of events, files accessed and the programs/utilities used. Monitoring of unauthorized access attempts include failed or rejected user actions, including attempts to access deactivated accounts, actions involving data and other resources, access policy violations, notification for network gateways and firewalls, and alerts from proprietary intrusion detection/protection systems (IDS/IPS). Monitoring of system alerts or failures include console alerts or messages, system log exceptions, network management alarms, alarms raised by the access control system (e.g., IDS/IPS or network monitoring software), and changes or attempts to change system security settings and controls.</p>	
47	<p>1215.09ab2System.7 - Auditing and monitoring systems employed by the organization support audit reduction and report generation.</p>	<p>DuploCloud installs by default Wazuh agent and AWS Inspector and any other Agent modules in all VMs and keeps them active. In case any node is failing the auto install DC raises an alarm. In Wazuh the alerts are configured and generated. We rely on customer's SOC team to act on the alerts. DuploCloud team is the second line of defense if the issue cannot be addressed by client team</p>
48	<p>1240.09aa2System.56 - The organization provides a rationale for why the auditable events are deemed adequate to support after-the-fact investigations of security incidents and</p>	<p>DuploCloud provides a document detailing the rationale and example of how the attributes of the audit trail are used in an after-the-fact investigation.</p>

	<p>which events require auditing on a continuous basis in response to specific situations.</p> <p>The listing of auditable events are reviewed and updated periodically within every 365 days.</p>	
49	<p>1271.09ad2System.1 - An intrusion detection system managed outside of the control of system and network administrators is used to monitor system and network administration activities for compliance.</p>	<p>DuploCloud orchestrates AWS Traffic mirroring to send a copy of the traffic at all critical points (tenants) to a Suricata VM. From there the alerts are fetched by Wazuh and displayed in the central dashboard. This provides IDS but if prevention is desired then the Suricata software is enabled in each critical VM preferably in the AMI (Image) itself. The alerts are then fetched by the Wazuh agent and updated in Wazuh SIEM</p>
50	<p>1208.09aa3System.1 - Audit logs are maintained for account management activities, system/server shutdown and reboot, system/server alerts and errors, application/system shutdown and reboot, application errors and modifications, file changes (create, update, delete), security policy changes, configuration changes, modification to sensitive information, read access to sensitive information, and printing of sensitive information.</p>	<p>DuploCloud, the platform, produces an audit trail of every action taken in the system. Additionally, all hosts created by DuploCloud will have auditing enabled at the operating system level.</p>
51	<p>1209.09aa3System.2 - The information system generates audit records containing the following detailed information: filename accessed; program or command used to initiate the event; source addresses; and destination addresses.</p>	<p>DuploCloud, the platform, produces an audit trail of every action taken in the system. Additionally, all hosts created by DuploCloud will have auditing enabled at the operating system level.</p>
52	<p>1216.09ab3System.12 - Automated systems are used to review monitoring activities on a daily basis for those servers that perform security functions (e.g., IDS/IPS) for:</p>	<p>DuploCloud installs by default Wazuh agent and AWS Inspector and any other Agent modules in all VMs and keeps them active. In case any node is failing the auto install DC raises an alarm. In Wazuh the alerts are configured and generated. We rely on customer's SOC team to act on the alerts. DuploCloud team is the second</p>

	<p>all security events; logs of all critical system components; and logs of all servers that perform security functions like intrusion detection system (IDS), intrusion prevention system (IPS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). System records are reviewed daily for initialization sequences, log-ons and errors, system processes and performance, and system resources utilization. The results of system record reviews are used to determine anomalies on demand.</p>	<p>line of defense if the issue cannot be addressed by client team</p>
53	<p>1217.09ab3System.3 - The organization ensures automated alerts are generated for technical personnel to review and analyze, and suspicious activity or suspected violations are investigated as an integrated part of the organization's formal incident response and investigations program.</p>	<p>DuploCloud installs by default Wazuh agent and AWS Inspector and any other Agent modules in all VMs and keeps them active. In case any node is failing the auto install DC raises an alarm. In Wazuh the alerts are configured and generated. We rely on customer's SOC team to act on the alerts. DuploCloud team is the second line of defense if the issue cannot be addressed by client team</p>
54	<p>1218.09ab3System.47 - Automated tools support near real-time analysis of events and maintain an audit log to track prohibited sources and services. Information systems provide near real-time alerts for the presence of malicious code, unauthorized export of information, signaling to an external information system, or potential intrusions.</p>	<p>SIEM, IDS, and IPS are all implemented out of the box</p>
55	<p>1219.09ab3System.10 - The information system</p>	<p>Duplo orchestrates with Wazuh as the SIEM which includes an interface for querying based on selectable criteria</p>

	is able to automatically process audit records for events of interest based on selectable criteria.	
56	<p>1220.09ab3System.56 - The organization ensures inbound and outbound communications are monitored at an organization-defined frequency for unusual or unauthorized activities or conditions. Change detection mechanisms (e.g., file-integrity monitoring tools) are used to alert personnel to unauthorized modification of critical system files, configuration files, or content files. Critical file comparisons are conducted at least weekly and the organization responds to any alerts generated.</p>	DuploCloud installs by default Wazuh agent and AWS Inspector and any other Agent modules in all VMs and keeps them active. In case any node is failing the auto install DC raises an alarm. In Wazuh the alerts are configured and generated. We rely on customer's SOC team to act on the alerts. DuploCloud team is the second line of defense if the issue cannot be addressed by client team
57	<p>1222.09ab3System.8 - The organization analyzes and correlates audit records across different repositories using a security information and event management (SIEM) tool or log analytics tools for log aggregation and consolidation from multiple systems/machines/devices, and correlates this information with input from non-technical sources to gain and enhance organization-wide situational awareness. Using the SIEM tool, the organization (system administrators and security personnel) devise profiles of common events from given systems/machines/devices so that it can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analyst with insignificant alerts.</p>	Duplo orchestrates with Wazuh as the SIEM. Wazuh agents are automatically installed in the hosts and is integrated with various services like CloudWatch, CloudTrail, AWS Inspector and Suricata. Which collects the vulnerabilities, and all of those vulnerabilities can be view in one page.

	18 Physical & Environmental Security	
58	1857.08c1Organizational.1 - Relevant health and safety regulations and standards are taken into consideration when securing facilities.	Inherited from the Cloud Service Provider
59	1871.08f1Organizational.13 - Access to a delivery and loading area from outside of the building is restricted to identified and authorized personnel. The external doors of a delivery and loading area are secured when the internal doors are opened.	Inherited from the Cloud Service Provider
60	1880.08g1Organizational.6 - The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, and considers the physical and environmental hazards in its risk mitigation strategy.	Inherited from the Cloud Service Provider, multiple Availability Zones and Regions are available
61	1888.08h1Organizational.456 - An uninterruptable power supply (UPS) to support orderly close down is required for equipment supporting critical business operations. Power contingency plans cover the action to be taken on failure of the UPS. The organization ensures UPS equipment and generators are regularly checked to ensure they have adequate capacity and are tested in accordance with the manufacturer's recommendations.	Inherited from the Cloud Service Provider
62	1899.08i1Organizational.1 - The organization protects power equipment and	Inherited from the Cloud Service Provider

	power cabling for the information system from damage and destruction.	
63	1803.08b2Organizational.10 - Repairs or modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors, and locks) are documented and retained in accordance with the organization's retention policy.	Inherited from the Cloud Service Provider
64	18131.09p2Organizational.3 - Media is disposed in a manner commensurate with the sensitivity of the information contained on the media using generally accepted and secure disposal or erasure methods for media that contains (or might contain) covered and/or confidential information. Procedures for the secure disposal of media containing information address the identification of information that qualifies as covered (otherwise a policy is developed that all information is considered covered in the absence of unequivocal evidence to the contrary).	Inherited from the Cloud Service Provider
65	1825.08l2Organizational.1 - The organization: ensures disk wiping or degaussing is used to securely remove electronic information; ensures shredding, disintegration, grinding surfaces, incineration, pulverization, or melting are used to destroy electronic and hard copy media; ensures devices containing covered and/or confidential information are physically destroyed or the information is destroyed, deleted, or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function;	Inherited from the Cloud Service Provider



	<p>renders information unusable, unreadable, or indecipherable on digital system media prior to disposal or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies;</p> <p>renders information unusable, unreadable, or indecipherable on non-digital system media prior to disposal or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies;</p> <p>destroys media containing covered and/or confidential information that cannot be sanitized.</p>	
	19 Data Protection & Privacy	
66	<p>19165.07e1Organizational.13 - The organization physically and/or electronically labels and handles sensitive information commensurate with the risk of the information or document.</p> <p>Labeling reflects the classification according to the rules in the information classification policy.</p>	Tags can be applied either at the Tenant or Resource level to identify the risk