cloudneeti

Stay secure. Stay compliant.

Product Capabilities

A Gartner recognized cloud security and compliance product company dedicated to identifying and eliminating cloud risks

May 2019

Agenda

01 Overview

Product Overview

02 Use cases

Product Use cases

03 Capabilities

Product Capabilities and Screenshots

Product Overview

Problem: Businesses are struggling with security and compliance impeding their public cloud adoption

Preventable cloud misconfigurations cause major data breaches

DEPARTMENT OF DEFENSE · UNITED STATES OF AMERICA

REPUBLICAN NATIONAL COMMITTEE

GoDaddy

W

broadsoft

verizon✓

accenture

Booz | Allen | Hamilton

TimeWarner

Source: *Various 2018 and 2019 data leak reports*

Fear of security mismanagement & mistakes delays cloud projects

Regulated projects delayed

Traditional tools don't work

Proving compliance is difficult

2018 Cloud Security Report, Cybersecurity Insiders ; Cloud Security Alliance top issues

91%

CISOs
concerned with

Prevent breaches + **Assure Compliance**

Solution: A SaaS product that proactively identifies and eliminates cloud risks

Visibility

Of security and compliance posture for multi-cloud workloads

Enforcement

Of standards using various remediations techniques

Continuous Governance

By managing and adjusting security posture

80% reduction

Risk of security breaches

-Gartner

30% faster

Secure cloud adoption

- Customers

50% reduction

Time to compliance

- Audit partners

Gartner recommends Cloud Security Posture Management (CSPM) as a top 10 security initiatives for 2019

Gartner®

> " Nearly all successful attacks on cloud services are the result of customer misconfiguration, mismanagement and mistakes.
>
> Organizations implementing a CSPM offering and extending this into development will reduce cloud-related security incidents due to misconfiguration by **80%.** "

-Gartner, Innovation Insight for Cloud Security Posture Management, 25 January 2019

Product: Continuous cloud security and compliance assurance

Azure

Office 365

amazon web services

Google Cloud

(roadmap)

Collect

Pull out actual cloud workload configuration

agentless

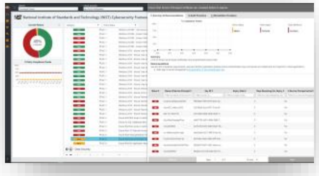
Analyze

Signature and ML based policy engine

IaaS, PaaS, Serverless, Kubernetes, Server OS, SaaS

Visibility

for 1100 security best practices across 12 frameworks

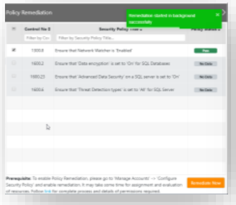


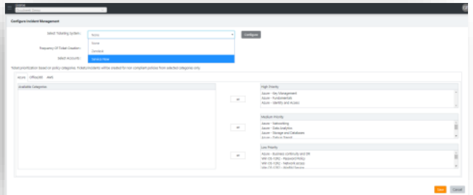
Prioritize Risks

Using ML infused risk likelihood

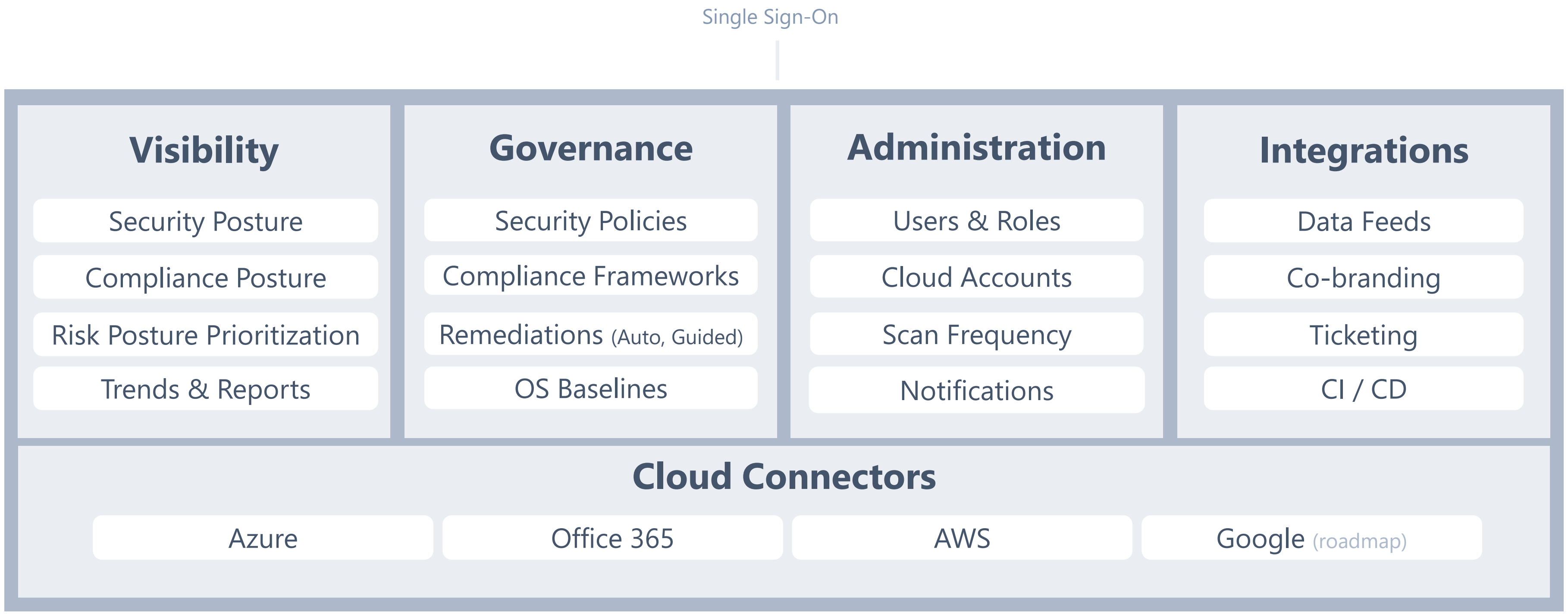
Fix Misconfigurations

Enforce via auto/guided remediations, CI/CD integrations





Features: Enable proactive management of cloud risks



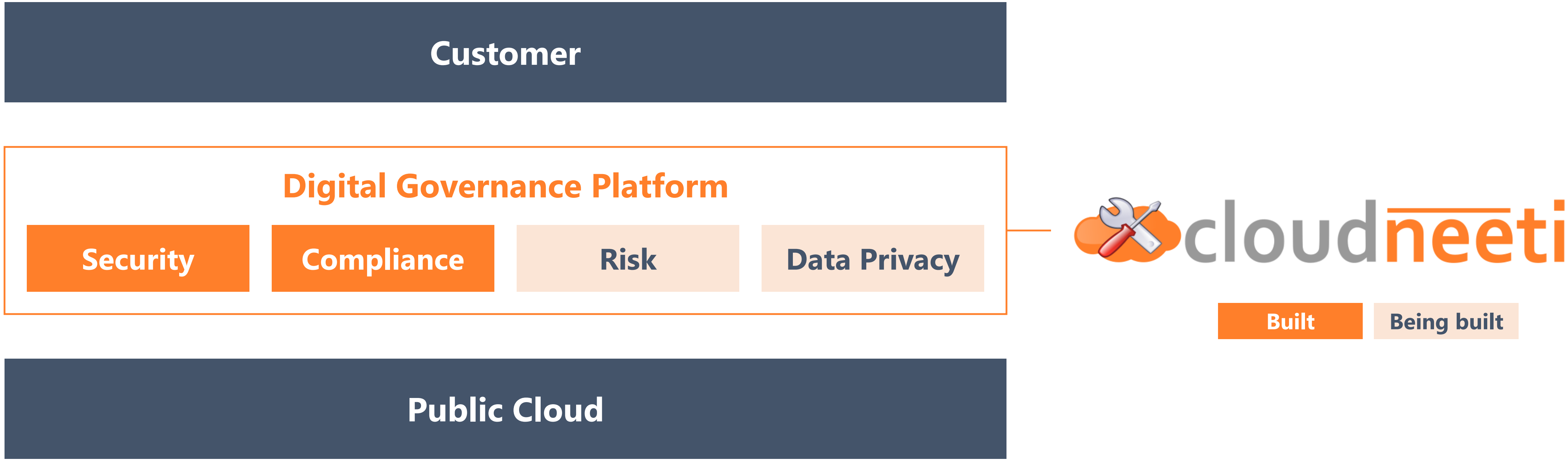
Single Sign-On

Visibility	Governance	Administration	Integrations
Security Posture	Security Policies	Users & Roles	Data Feeds
Compliance Posture	Compliance Frameworks	Cloud Accounts	Co-branding
Risk Posture Prioritization	Remediations (Auto, Guided)	Scan Frequency	Ticketing
Trends & Reports	OS Baselines	Notifications	CI / CD

Cloud Connectors

Azure	Office 365	AWS	Google (roadmap)

Vision: The Digital Governance Platform for Security and Risk



Customer

Digital Governance Platform

Security

Compliance

Risk

Data Privacy

Public Cloud

cloudneeti

Built

Being built

Coverage: Unprecedented breadth and depth of coverage

Breadth and Depth of Coverage

				product roadmap
Cloud Services Providers	Azure		amazon web services	Google Cloud Platform
— Cloud Services	IaaS	PaaS	Serverless	Containers
— Operating Systems	Windows Server			Linux
Software as a Service	Microsoft 365			salesforce Microsoft Dynamics 365

Cloudneeti provides continuous assurance for multiple security and compliance standards

Security and Compliance Standards

Security

NIST National Institute of Standards and Technology
Cybersecurity Framework

CIS Center for Internet Security®

CSA cloud security alliance®

Compliance

NIST National Institute of Standards and Technology
800-53 r4 / FISMA

ISO 27001
International Organization for Standardization

PCI Data Security Standard V 3.2

HIPAA COMPLIANCE

AICPA SOC

FFIEC

UK NCSC

Reserve Bank Of India

General Data Protection Regulation

GxP
Life Sciences

Cloudneeti is recognized by the cloud security professional community

Industry Recognitions & Certifications

Gartner

Recognized CSPM vendor

Innovation Insight for Cloud Security Posture Management – Neil MacDonald, 25 January 2019

CIS

Certified by CIS

A CIS Secure Suite product vendor and an author for many cloud benchmarks
https://www.cisecurity.org/partner/cloudneeti/

AICPA SOC

SOC2 certified Organization

Organizational controls attested by 3rd party AICPA auditor

Deep Cloud Service Provider Relationships

Microsoft

Validation engine for Azure Blueprints

Secure and compliant solutions to help organizations adopt cloud securely
https://aka.ms/azureblueprint

Microsoft For Startups

Microsoft Azure Certified

Microsoft Azure certified ISV and groomed by Microsoft for Startups

Azure for Healthcare
Azure for Financial Services
Azure Security Center

amazon web services | Partner Network
TECHNOLOGY PARTNER

An AWS Technology partner ISV

Product Use cases

Cloudneeti enables secure cloud adoption scenarios

Cloudneeti Focus Areas

Workload Configuration Security

IaaS, PaaS, Serverless, Database, Storage, Data analytics, Networking, Workload IAM settings, Kubernetes and more

Cloud Account Security

Root account settings, Account IAM settings, Monitoring profiles, Security center/hub configurations

Compliance Frameworks

12 Compliance Frameworks: e.g. PCI DSS, HIPAA, SOC2, ISO 27001, FFIEC CAT, NIST, GxP and more.

Customer Usage Scenarios

Cloud Migration & Continuous Operations

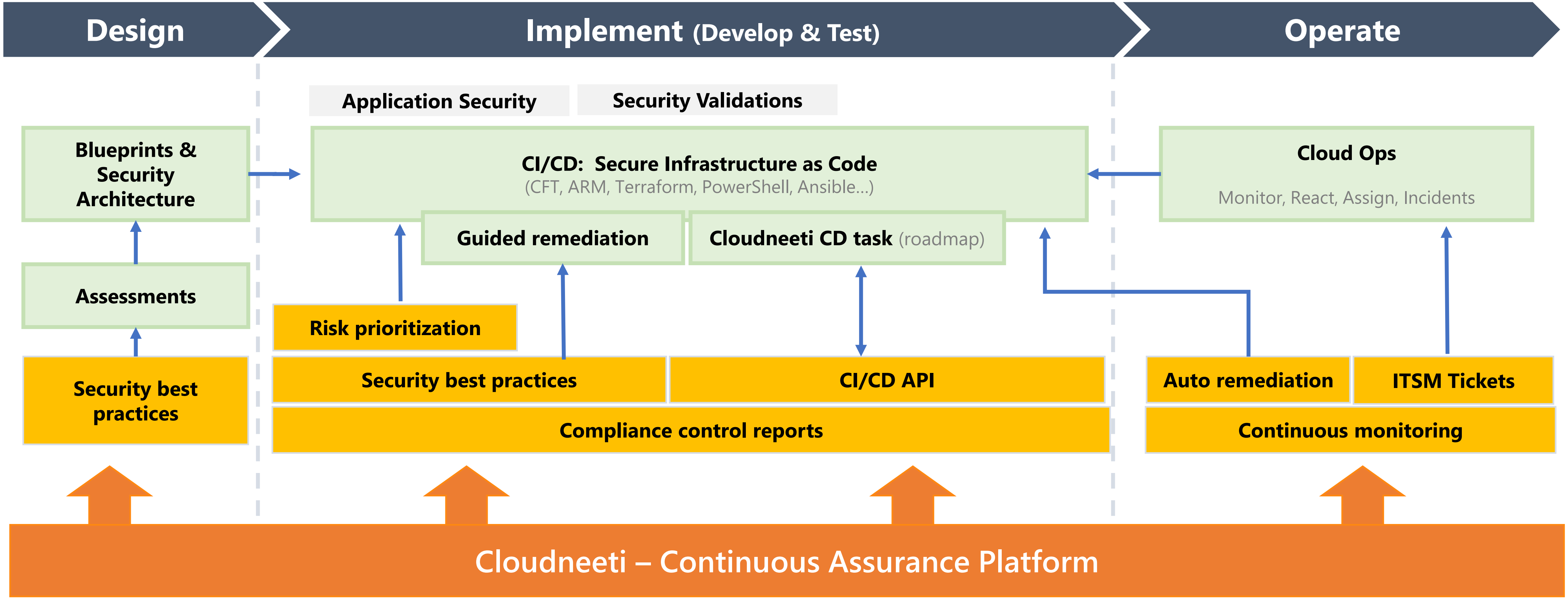
Advisory & Managed Services

Continuous Risk and Compliance Audits

Cloudneeti influenced DevSecOps

Customer Actions

Cloudneeti Output



Design

Implement (Develop & Test)

Operate

Application Security

Security Validations

Blueprints & Security Architecture

CI/CD: Secure Infrastructure as Code

(CFT, ARM, Terraform, PowerShell, Ansible…)

Cloud Ops

Monitor, React, Assign, Incidents

Guided remediation

Cloudneeti CD task (roadmap)

Assessments

Risk prioritization

Security best practices

Security best practices

CI/CD API

Auto remediation

ITSM Tickets

Compliance control reports

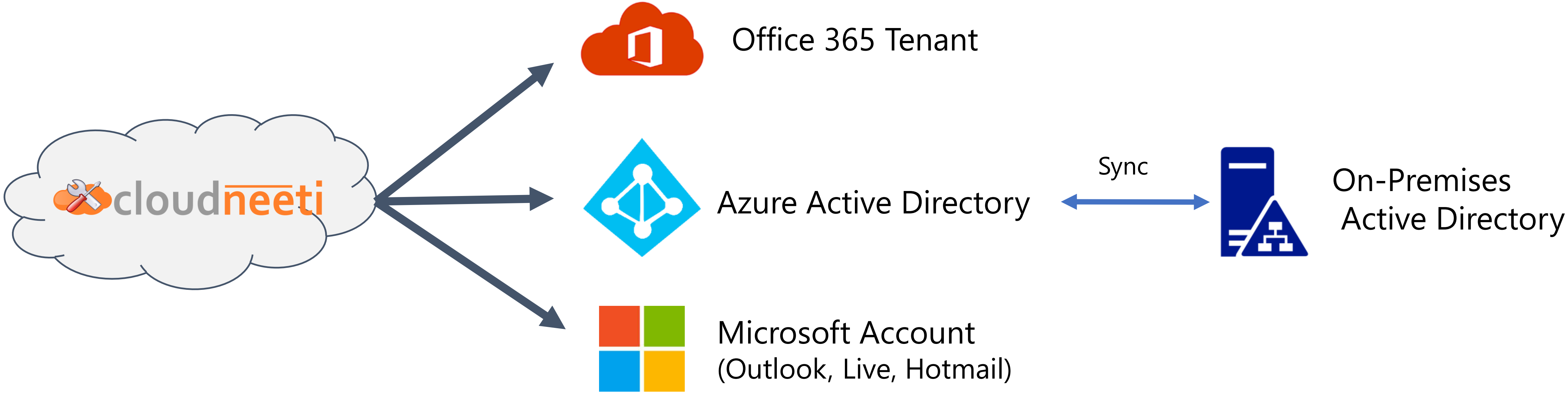
Continuous monitoring

Cloudneeti – Continuous Assurance Platform

Product Capabilities and Screenshots

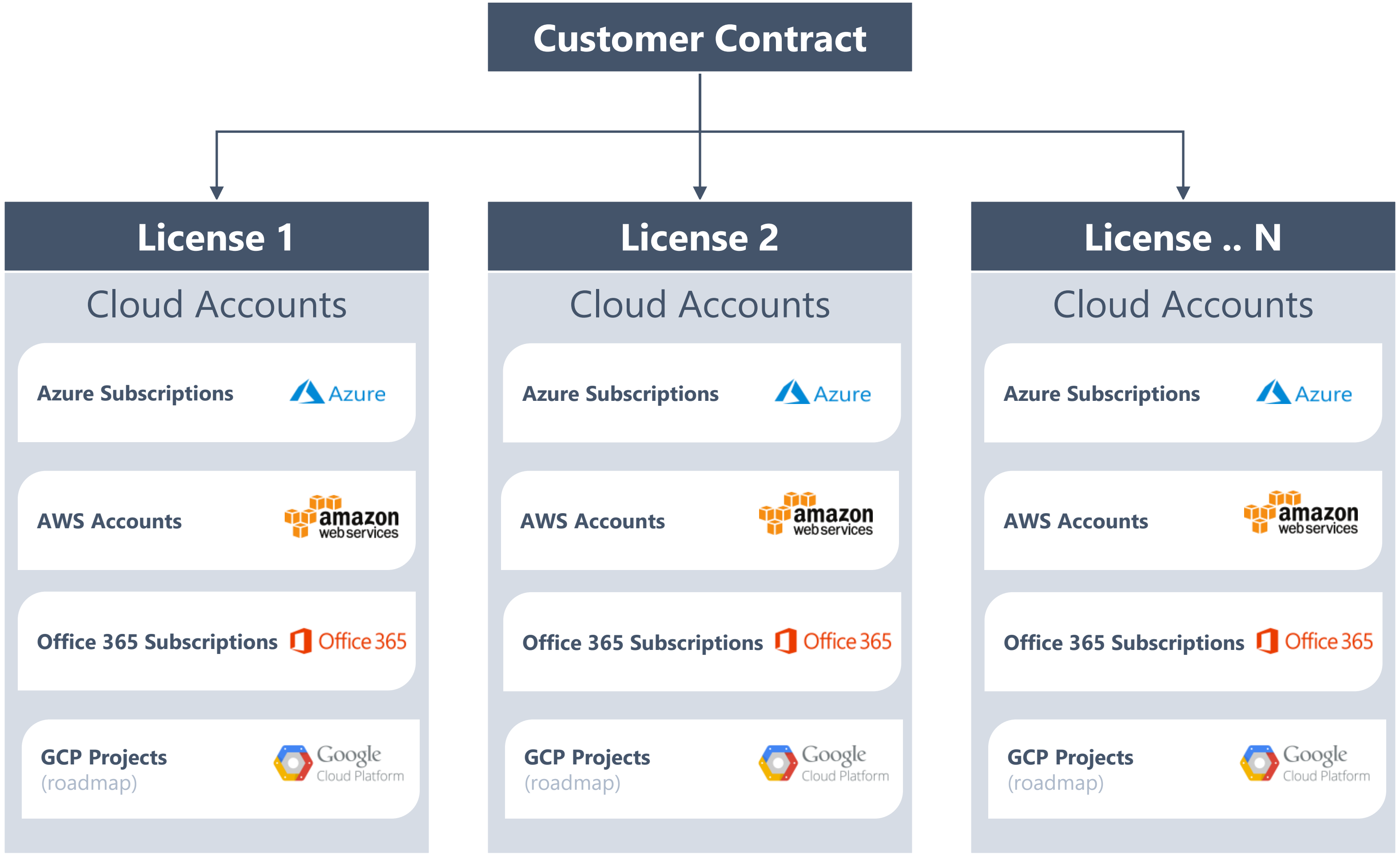
SSO Authentication: Cloudneeti uses SSO to authenticate with Customer's preferred Identity Provider

Cloudneeti does not manage Users and Passwords. Instead allows for SSO (Single Sign On) with Microsoft Azure AD, Office 365, Microsoft Accounts (Outlook, Hotmail, Live)



Cloudneeti secures workloads across multiple cloud providers

cloudneeti



Customer Contract

License 1

Cloud Accounts

Azure Subscriptions — Azure

AWS Accounts — amazon web services

Office 365 Subscriptions — Office 365

GCP Projects (roadmap) — Google Cloud Platform

License 2

Cloud Accounts

Azure Subscriptions — Azure

AWS Accounts — amazon web services

Office 365 Subscriptions — Office 365

GCP Projects (roadmap) — Google Cloud Platform

License .. N

Cloud Accounts

Azure Subscriptions — Azure

AWS Accounts — amazon web services

Office 365 Subscriptions — Office 365

GCP Projects (roadmap) — Google Cloud Platform

Note: Cloud Account means an Azure/O365/AWS/GCP cloud provider subscription/account/project.

Ticketing: Incident Management

Organization need tickets to raised automatically for any deviations from baseline security posture.

Cloudneeti supports IT integration with enterprise level Ticketing/Incident Management system.

Notifications support available for tickets raised.

Cloudneeti supports for customization such as classification, prioritization (High/Medium/Low) of Tickets.

Ticketing System supported include ZenDesk and ServiceNow.
Future support planned for Jira and Azure DevOps

Supported

zendesk servicenow

Planned

JIRA Azure DevOps

Data Feeds: Reporting Data Feeds

Organization create customized dashboard/reports for Security and Compliance requirement for different personas as per their business mandates.

Cloudneeti supports integration with your organization reporting platforms such as Tableau/Power BI/Qlikview using Data Feed for security & compliance data.

Data Feed Repository supported include Storage Accounts & Cosmos DB

Customization available for Data Feed Frequency are Daily, Weekly or Monthly

Notification supported for Cloudneeti notifies License Admin for any connection while Data Feed.

Data Feed format is JSON

Supported

Blob Storage

Azure Cosmos DB storage

Planned

amazon S3

Integrations: Auditing Logs Data Feeds

Organization need to provide data of system & user activities for compliance.

Cloudneeti support audit logging to provide records of system & user activities for compliance.

Cloudneeti support data feed for audit to Organization own repositories such as Storage Account and Cosmos DB.

Auditing is always on by default and can be viewed on Cloudneeti Portal

Full text Search is available on Audit logs.

An audit log has a default list view that shows:

- The activity description
- The target Contract Name
- The target Account Name
- The date and time of the occurrence
- The initiator / actor (*who*) of an activity
- The activity (*what*)

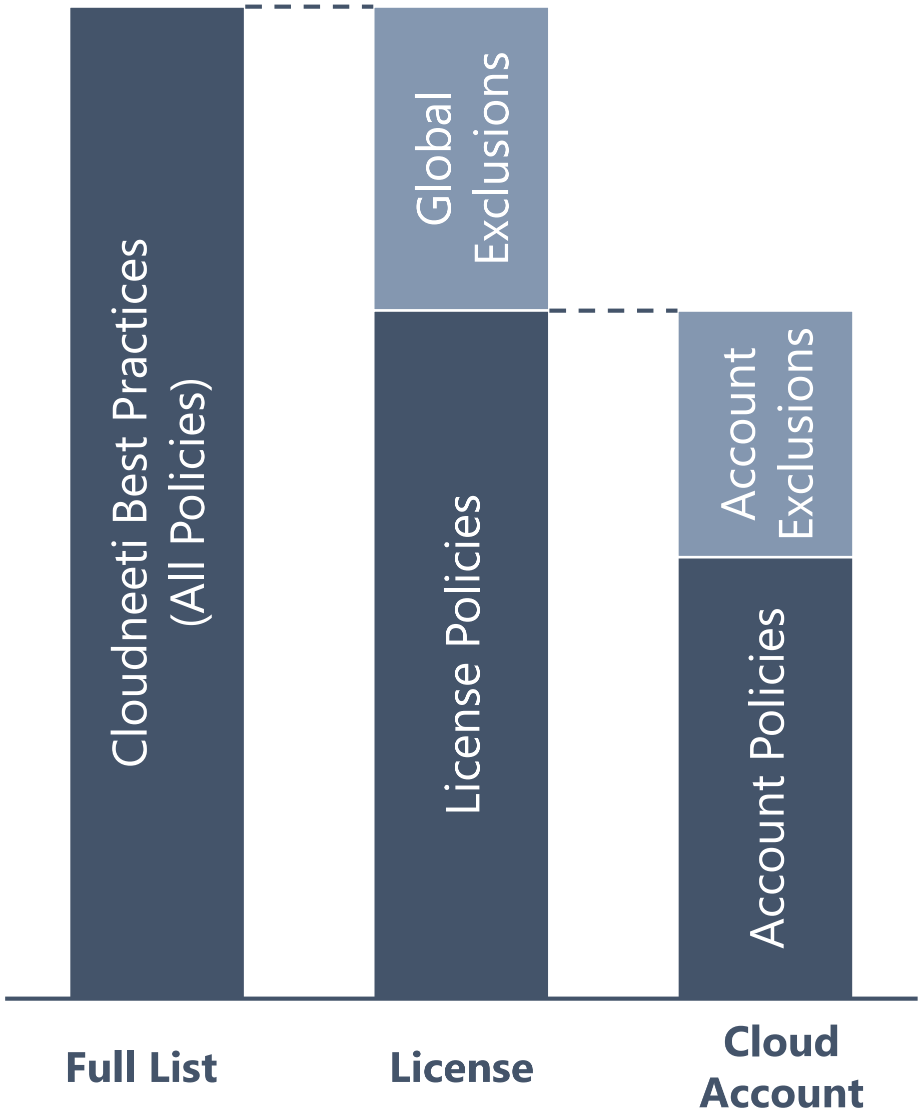
Policy Exceptions: Allowances to tune Organizational policies

Organization can customize the available policies from Cloudneeti as per their needs. Depending on the Cloud resources deployed, enterprises can apply the relevant policies for organizational InfoSec governance among the hundreds of policies available.

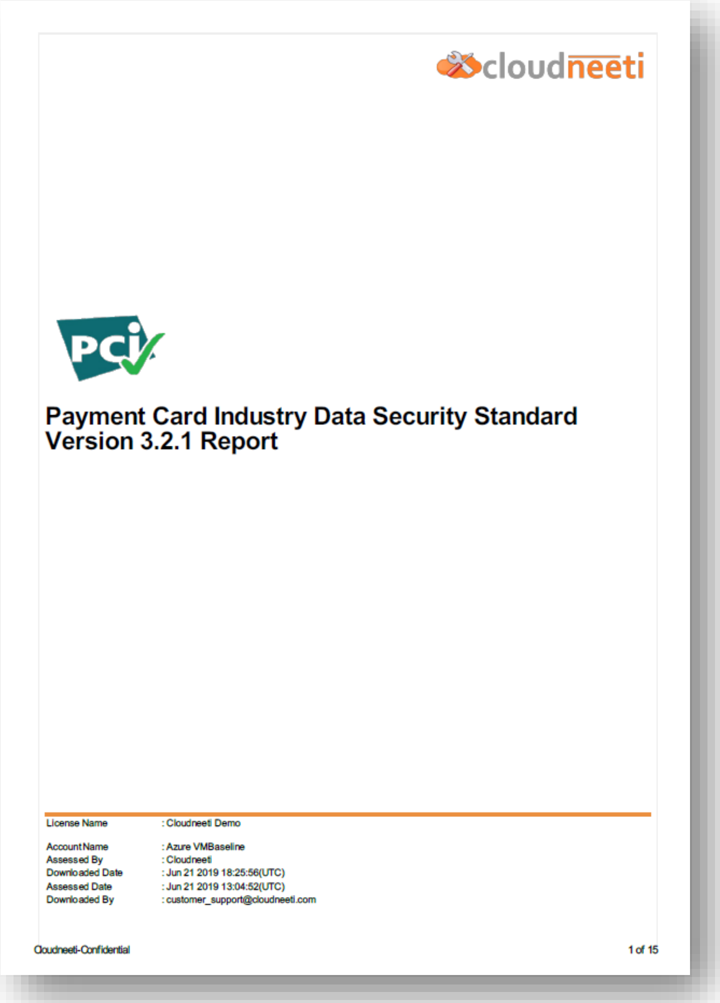
Cloudneeti supports policies configuration/ exception at License level as the top level.

Next level of policy exception support is available at Cloud Account level.

Policies excluded at the License level will be automatically excluded at the Account Level.



Reports: 1-click downloadable reports for Security & Compliance Posture

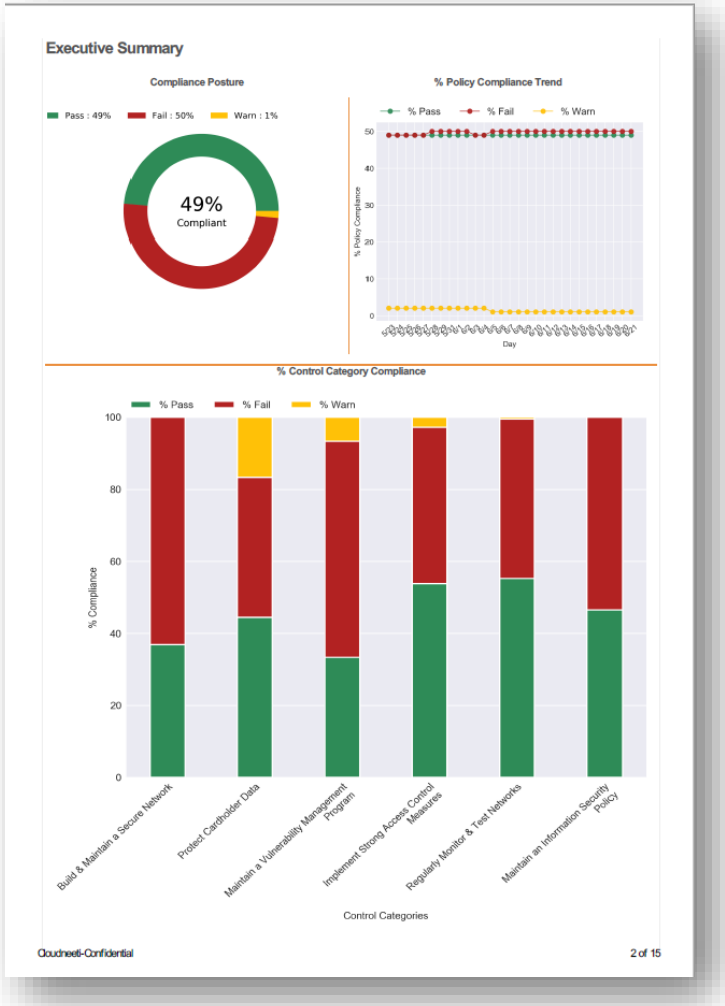


cloudneeti

Payment Card Industry Data Security Standard Version 3.2.1 Report

License Name	: Cloudneeti Demo
Account Name	: Azure VMBaseline
Assessed By	: Cloudneeti
Downloaded Date	: Jun 21 2019 18:25:56(UTC)
Assessed Date	: Jun 21 2019 13:04:52(UTC)
Downloaded By	: customer_support@cloudneeti.com

Cloudneeti-Confidential 1 of 15



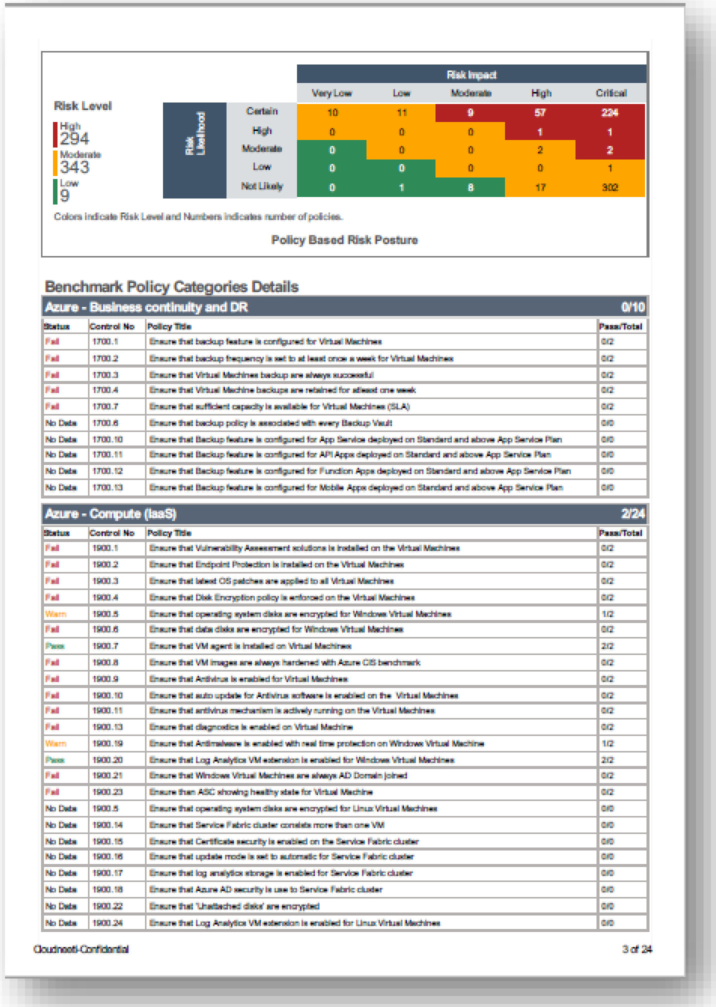
Executive Summary

Compliance Posture

% Policy Compliance Trend

% Control Category Compliance

Cloudneeti-Confidential 2 of 15



Risk Level

- High 294
- Moderate 343
- Low 9

		Risk Impact				
		Very Low	Low	Moderate	High	Critical
Risk Likelihood	Certain	10	11	9	57	224
	High	0	0	0	1	1
	Moderate	0	0	0	2	2
	Low	0	0	0	0	1
	Not Likely	0	1	8	17	302

Colors indicate Risk Level and Numbers indicates number of policies.

Policy Based Risk Posture

Benchmark Policy Categories Details

Azure - Business continuity and DR 0/10

Status	Control No	Policy Title	Pass/Total
Fail	1700.1	Ensure that backup feature is configured for Virtual Machines	0/2
Fail	1700.2	Ensure that backup frequency is set to at least once a week for Virtual Machines	0/2
Fail	1700.3	Ensure that Virtual Machines backup are always successful	0/2
Fail	1700.4	Ensure that Virtual Machine backups are retained for atleast one week	0/2
Fail	1700.7	Ensure that sufficient capacity is available for Virtual Machines (SLA)	0/2
No Data	1700.6	Ensure that backup policy is associated with every Backup Vault	0/0
No Data	1700.10	Ensure that Backup feature is configured for App Service deployed on Standard and above App Service Plan	0/0
No Data	1700.11	Ensure that Backup feature is configured for API Apps deployed on Standard and above App Service Plan	0/0
No Data	1700.12	Ensure that Backup feature is configured for Function Apps deployed on Standard and above App Service Plan	0/0
No Data	1700.13	Ensure that Backup feature is configured for Mobile Apps deployed on Standard and above App Service Plan	0/0

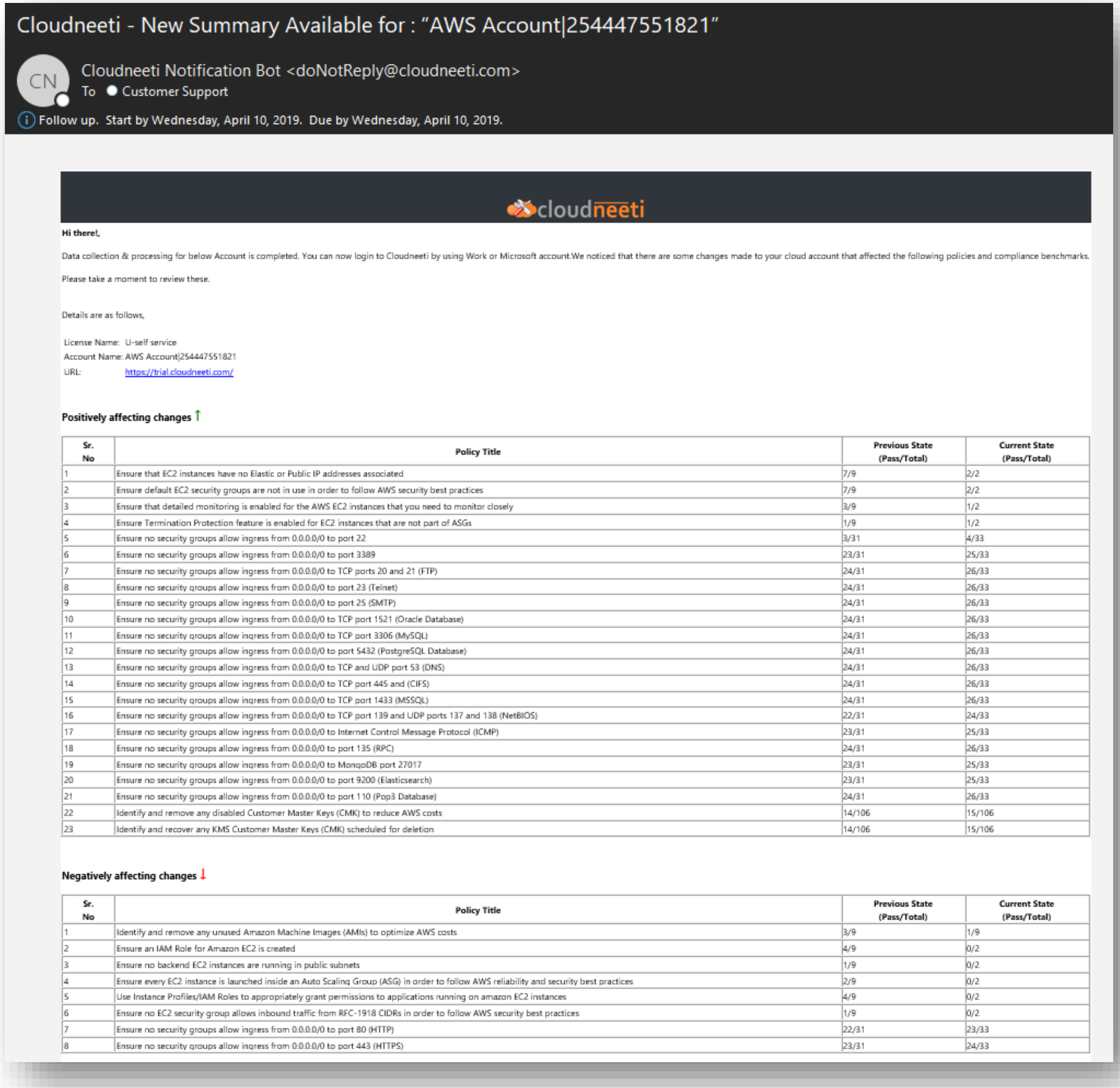
Azure - Compute (IaaS) 2/24

Status	Control No	Policy Title	Pass/Total
Fail	1900.1	Ensure that Vulnerability Assessment solutions is installed on the Virtual Machines	0/2
Fail	1900.2	Ensure that Endpoint Protection is installed on the Virtual Machines	0/2
Fail	1900.3	Ensure that latest OS patches are applied to all Virtual Machines	0/2
Fail	1900.4	Ensure that Disk Encryption policy is enforced on the Virtual Machines	0/2
Warn	1900.5	Ensure that operating system disks are encrypted for Windows Virtual Machines	1/2
Fail	1900.6	Ensure that data disks are encrypted for Windows Virtual Machines	0/2
Pass	1900.7	Ensure that VM agent is installed on Virtual Machines	2/2
Fail	1900.8	Ensure that VM images are always hardened with Azure CIS benchmark	0/2
Fail	1900.9	Ensure that Antivirus is enabled for Virtual Machines	0/2
Fail	1900.10	Ensure that auto update for Antivirus software is enabled on the Virtual Machines	0/2
Fail	1900.11	Ensure that antivirus mechanism is actively running on the Virtual Machines	0/2
Fail	1900.13	Ensure that diagnostics is enabled on Virtual Machine	0/2
Warn	1900.19	Ensure that Antimalware is enabled with real time protection on Windows Virtual Machine	1/2
Pass	1900.20	Ensure that Log Analytics VM extension is enabled for Windows Virtual Machines	2/2
Fail	1900.21	Ensure that Windows Virtual Machines are always AD Domain joined	0/2
Fail	1900.23	Ensure than ASC showing healthy state for Virtual Machine	0/2
No Data	1900.5	Ensure that operating system disks are encrypted for Linux Virtual Machines	0/0
No Data	1900.14	Ensure that Service Fabric cluster consists more than one VM	0/0
No Data	1900.15	Ensure that Certificate security is enabled on the Service Fabric cluster	0/0
No Data	1900.16	Ensure that update mode is set to automatic for Service Fabric cluster	0/0
No Data	1900.17	Ensure that log analytics storage is enabled for Service Fabric cluster	0/0
No Data	1900.18	Ensure that Azure AD security is use to Service Fabric cluster	0/0
No Data	1900.22	Ensure that 'Unattached disks' are encrypted	0/0
No Data	1900.24	Ensure that Log Analytics VM extension is enabled for Linux Virtual Machines	0/0

Cloudneeti-Confidential 3 of 24

Notifications: Configurable Email notifications to alert on positively and negatively impacting changes

Notifications allow customers to monitor and react to security posture changes



Cloudneeti - New Summary Available for : "AWS Account|254447551821"

Cloudneeti Notification Bot <doNotReply@cloudneeti.com>
To ● Customer Support

Follow up. Start by Wednesday, April 10, 2019. Due by Wednesday, April 10, 2019.

Hi there!,

Data collection & processing for below Account is completed. You can now login to Cloudneeti by using Work or Microsoft account.We noticed that there are some changes made to your cloud account that affected the following policies and compliance benchmarks.

Please take a moment to review these.

Details are as follows,

License Name: U-self service
Account Name: AWS Account|254447551821
URL: https://trial.cloudneeti.com/

Positively affecting changes ↑

Sr. No	Policy Title	Previous State (Pass/Total)	Current State (Pass/Total)
1	Ensure that EC2 instances have no Elastic or Public IP addresses associated	7/9	2/2
2	Ensure default EC2 security groups are not in use in order to follow AWS security best practices	7/9	2/2
3	Ensure that detailed monitoring is enabled for the AWS EC2 instances that you need to monitor closely	3/9	1/2
4	Ensure Termination Protection feature is enabled for EC2 instances that are not part of ASGs	1/9	1/2
5	Ensure no security groups allow ingress from 0.0.0.0/0 to port 22	3/31	4/33
6	Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389	23/31	25/33
7	Ensure no security groups allow ingress from 0.0.0.0/0 to TCP ports 20 and 21 (FTP)	24/31	26/33
8	Ensure no security groups allow ingress from 0.0.0.0/0 to port 23 (Telnet)	24/31	26/33
9	Ensure no security groups allow ingress from 0.0.0.0/0 to port 25 (SMTP)	24/31	26/33
10	Ensure no security groups allow ingress from 0.0.0.0/0 to TCP port 1521 (Oracle Database)	24/31	26/33
11	Ensure no security groups allow ingress from 0.0.0.0/0 to TCP port 3306 (MySQL)	24/31	26/33
12	Ensure no security groups allow ingress from 0.0.0.0/0 to port 5432 (PostgreSQL Database)	24/31	26/33
13	Ensure no security groups allow ingress from 0.0.0.0/0 to TCP and UDP port 53 (DNS)	24/31	26/33
14	Ensure no security groups allow ingress from 0.0.0.0/0 to TCP port 445 and (CIFS)	24/31	26/33
15	Ensure no security groups allow ingress from 0.0.0.0/0 to TCP port 1433 (MSSQL)	24/31	26/33
16	Ensure no security groups allow ingress from 0.0.0.0/0 to TCP port 139 and UDP ports 137 and 138 (NetBIOS)	22/31	24/33
17	Ensure no security groups allow ingress from 0.0.0.0/0 to Internet Control Message Protocol (ICMP)	23/31	25/33
18	Ensure no security groups allow ingress from 0.0.0.0/0 to port 135 (RPC)	24/31	26/33
19	Ensure no security groups allow ingress from 0.0.0.0/0 to MongoDB port 27017	23/31	25/33
20	Ensure no security groups allow ingress from 0.0.0.0/0 to port 9200 (Elasticsearch)	23/31	25/33
21	Ensure no security groups allow ingress from 0.0.0.0/0 to port 110 (Pop3 Database)	24/31	26/33
22	Identify and remove any disabled Customer Master Keys (CMK) to reduce AWS costs	14/106	15/106
23	Identify and recover any KMS Customer Master Keys (CMK) scheduled for deletion	14/106	15/106

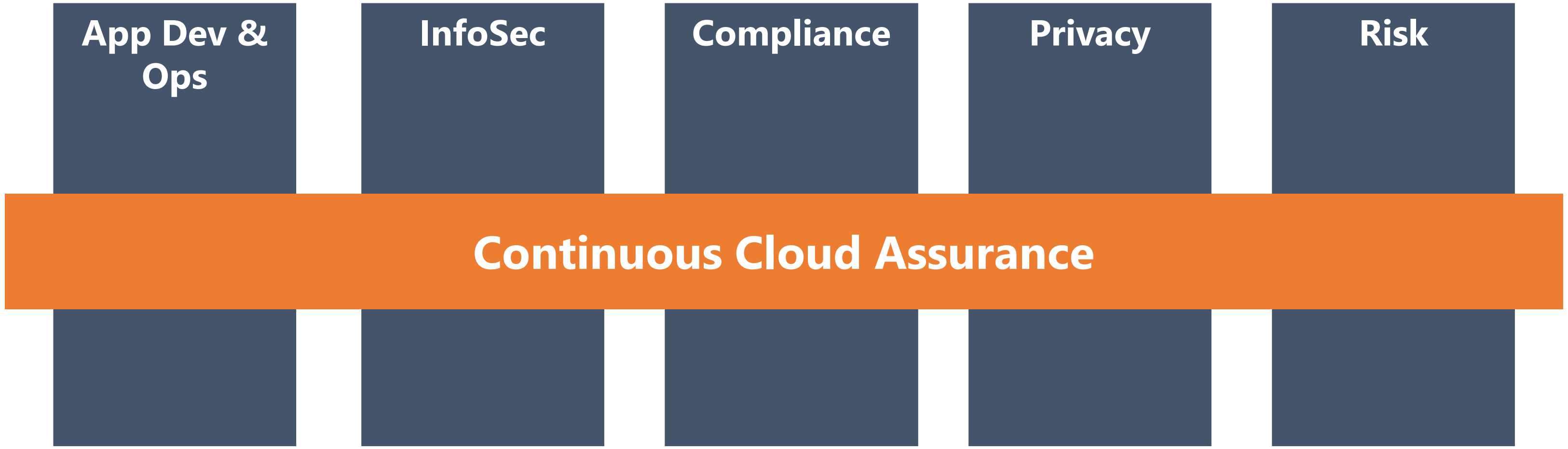
Negatively affecting changes ↓

Sr. No	Policy Title	Previous State (Pass/Total)	Current State (Pass/Total)
1	Identify and remove any unused Amazon Machine Images (AMIs) to optimize AWS costs	3/9	1/9
2	Ensure an IAM Role for Amazon EC2 is created	4/9	0/2
3	Ensure no backend EC2 instances are running in public subnets	1/9	0/2
4	Ensure every EC2 instance is launched inside an Auto Scaling Group (ASG) in order to follow AWS reliability and security best practices	2/9	0/2
5	Use Instance Profiles/IAM Roles to appropriately grant permissions to applications running on amazon EC2 instances	4/9	0/2
6	Ensure no EC2 security group allows inbound traffic from RFC-1918 CIDRs in order to follow AWS security best practices	1/9	0/2
7	Ensure no security groups allow ingress from 0.0.0.0/0 to port 80 (HTTP)	22/31	23/33
8	Ensure no security groups allow ingress from 0.0.0.0/0 to port 443 (HTTPS)	23/31	24/33

Use cases across the Enterprise

Transform entire Digital Risk Management Solutions Stack with Visibility, Enforcements and Ongoing Governance

Single console across security organizations



App Dev & Ops

InfoSec

Compliance

Privacy

Risk

Continuous Cloud Assurance

App Dev & Ops

- CI/CD
- Remediation guidance

InfoSec

- Best practices
- Multi-cloud Security Posture
- Enforcement mechanisms

Compliance

1-click reporting across 12+ Compliance frameworks

Privacy

- Data classification
- Data protection
- Access control assurance

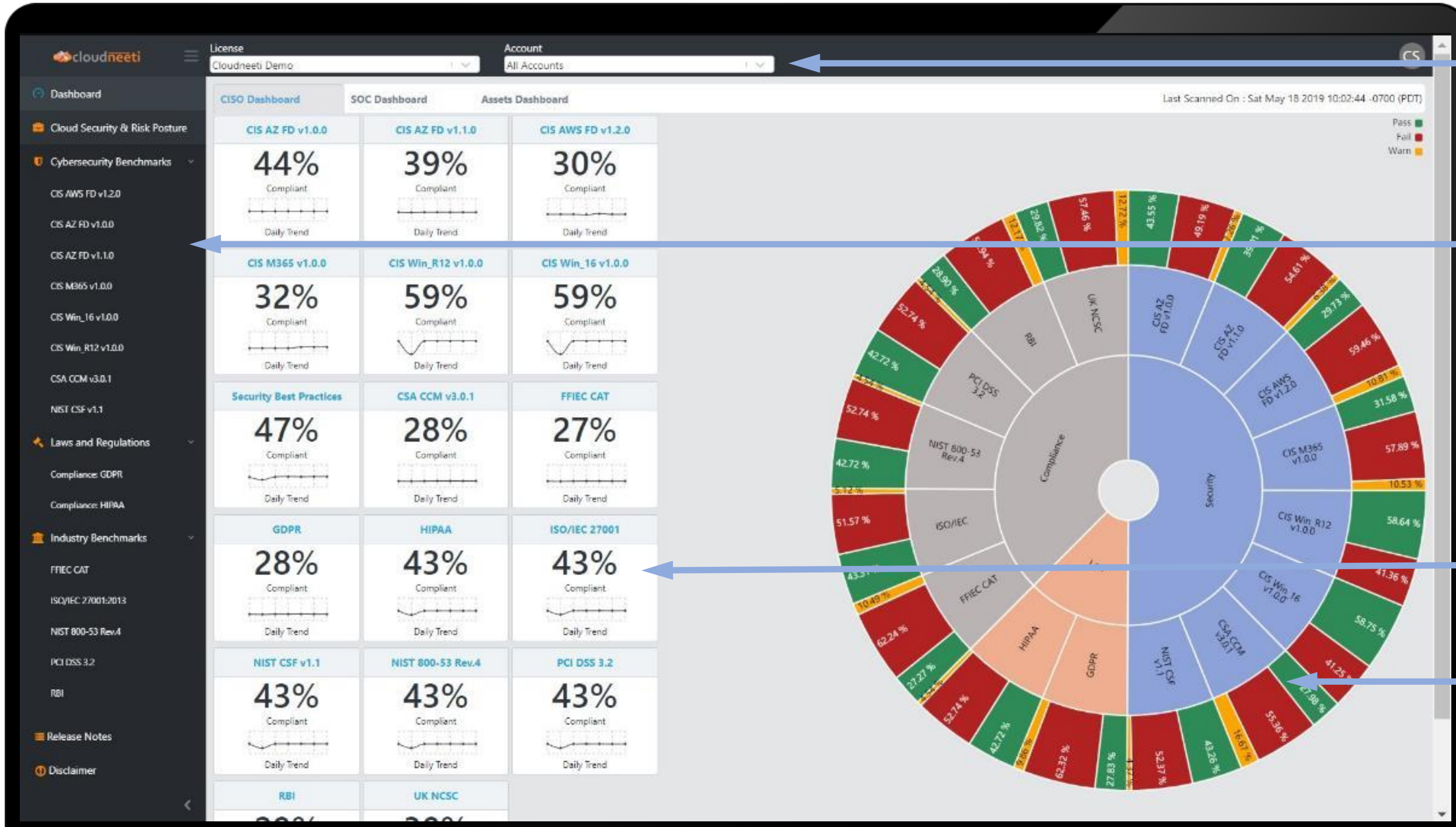
Risk

Digital risk (Cloud workloads)

- Visibility
- Prioritization matrix (impact vs likelihood)

Across organization

Dashboards displays cloud security and compliance posture



cloudneeti

License: Cloudneeti Demo

Account: All Accounts

- Dashboard
- Cloud Security & Risk Posture
- Cybersecurity Benchmarks
  - CIS AWS FD v1.2.0
  - CIS AZ FD v1.0.0
  - CIS AZ FD v1.1.0
  - CIS M365 v1.0.0
  - CIS Win_16 v1.0.0
  - CIS Win_R12 v1.0.0
  - CSA CCM v3.0.1
  - NIST CSF v1.1
- Laws and Regulations
  - Compliance: GDPR
  - Compliance: HIPAA
- Industry Benchmarks
  - FFIEC CAT
  - ISO/IEC 27001:2013
  - NIST 800-53 Rev.4
  - PCI DSS 3.2
  - RBI
- Release Notes
- Disclaimer

CISO Dashboard | SOC Dashboard | Assets Dashboard

Last Scanned On : Sat May 18 2019 10:02:44 -0700 (PDT)

CIS AZ FD v1.0.0 44% Compliant Daily Trend	CIS AZ FD v1.1.0 39% Compliant Daily Trend	CIS AWS FD v1.2.0 30% Compliant Daily Trend
CIS M365 v1.0.0 32% Compliant Daily Trend	CIS Win_R12 v1.0.0 59% Compliant Daily Trend	CIS Win_16 v1.0.0 59% Compliant Daily Trend
Security Best Practices 47% Compliant Daily Trend	CSA CCM v3.0.1 28% Compliant Daily Trend	FFIEC CAT 27% Compliant Daily Trend
GDPR 28% Compliant Daily Trend	HIPAA 43% Compliant Daily Trend	ISO/IEC 27001 43% Compliant Daily Trend
NIST CSF v1.1 43% Compliant Daily Trend	NIST 800-53 Rev.4 43% Compliant Daily Trend	PCI DSS 3.2 43% Compliant Daily Trend
RBI	UK NCSC	

Dashboard view is available across all/ individual cloud accounts. License is a way to aggregate monitoring and analysis at a group of cloud accounts.

Security Benchmarks:
CIS, NIST CSF, SOC2, CSA CCM;
Laws and Regulations:
GDPR, HIPAA;
Industry Benchmarks:
FFIEC, ISO 27001, NIST 800-53r4, PCI DSS, RBI, UK NCSC;

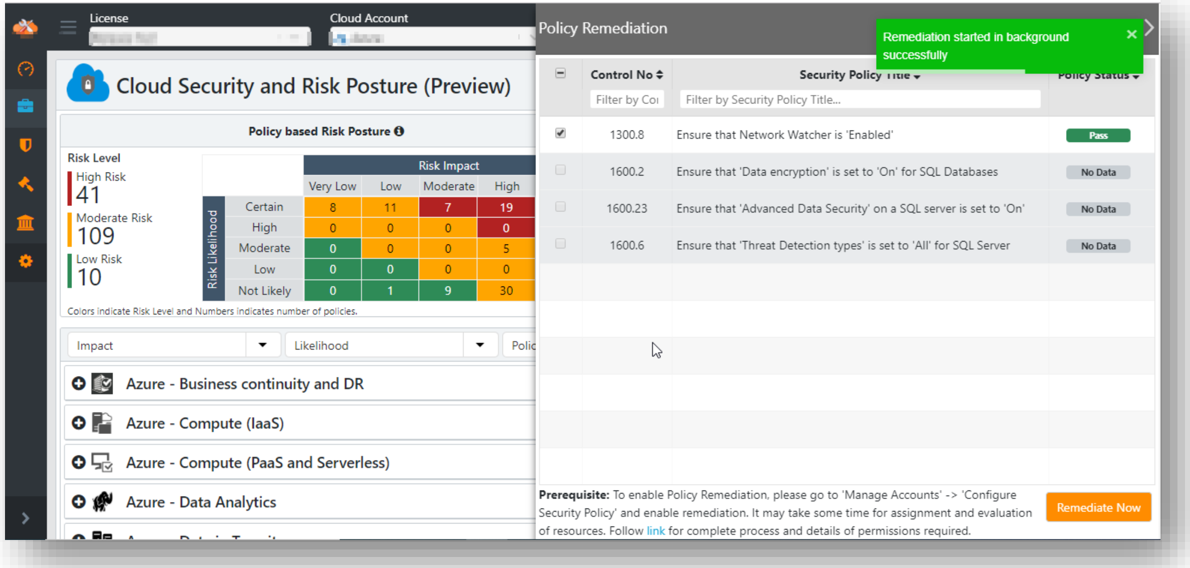
Aggregated security and compliance score across all cloud accounts

Sunburst view across 12 out of the box laws, compliance frameworks and security benchmarks

Remediations: Automated and Guided remediations

1-click auto remediations

for key Azure and AWS security configurations



License [redacted] Cloud Account [redacted]

Remediation started in background successfully

Cloud Security and Risk Posture (Preview)

Policy based Risk Posture

Risk Level

High Risk 41

Moderate Risk 109

Low Risk 10

Risk Likelihood	Very Low	Low	Moderate	High
	Risk Impact			
Certain	8	11	7	19
High	0	0	0	0
Moderate	0	0	0	5
Low	0	0	0	0
Not Likely	0	1	9	30

Colors indicate Risk Level and Numbers indicates number of policies.

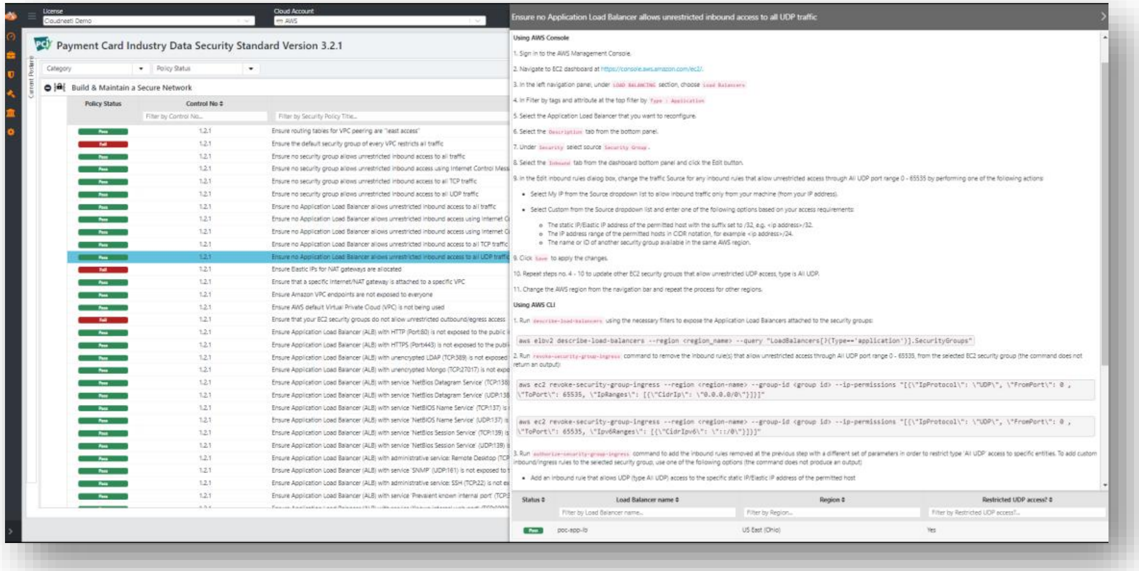
- Azure - Business continuity and DR
- Azure - Compute (IaaS)
- Azure - Compute (PaaS and Serverless)
- Azure - Data Analytics

☐	Control No	Security Policy Title	Policy Status
	Filter by Co	Filter by Security Policy Title...	
☑	1300.8	Ensure that Network Watcher is 'Enabled'	Pass
☐	1600.2	Ensure that 'Data encryption' is set to 'On' for SQL Databases	No Data
☐	1600.23	Ensure that 'Advanced Data Security' on a SQL server is set to 'On'	No Data
☐	1600.6	Ensure that 'Threat Detection types' is set to 'All' for SQL Server	No Data

Prerequisite: To enable Policy Remediation, please go to 'Manage Accounts' -> 'Configure Security Policy' and enable remediation. It may take some time for assignment and evaluation of resources. Follow link for complete process and details of permissions required.

Guided remediations

for all Azure and AWS security configurations



License: Cloudneeti Demo Cloud Account: AWS

Payment Card Industry Data Security Standard Version 3.2.1

Build & Maintain a Secure Network

Policy Status	Control No	
	Filter by Control No...	Filter by Security Policy Title...
Pass	1.2.1	Ensure routing tables for VPC peering are "least access"
Fail	1.2.1	Ensure the default security group of every VPC restricts all traffic
Pass	1.2.1	Ensure no security group allows unrestricted inbound access to all traffic
Pass	1.2.1	Ensure no security group allows unrestricted inbound access using Internet Control Mess
Pass	1.2.1	Ensure no security group allows unrestricted inbound access to all TCP traffic
Pass	1.2.1	Ensure no security group allows unrestricted inbound access to all UDP traffic
Pass	1.2.1	Ensure no Application Load Balancer allows unrestricted inbound access to all traffic
Pass	1.2.1	Ensure no Application Load Balancer allows unrestricted inbound access using Internet C
Pass	1.2.1	Ensure no Application Load Balancer allows unrestricted inbound access using Internet C
Pass	1.2.1	Ensure no Application Load Balancer allows unrestricted inbound access to all TCP traffic
Pass	1.2.1	Ensure no Application Load Balancer allows unrestricted inbound access to all UDP traffic
Fail	1.2.1	Ensure Elastic IPs for NAT gateways are allocated
Pass	1.2.1	Ensure that a specific Internet/NAT gateway is attached to a specific VPC
Pass	1.2.1	Ensure Amazon VPC endpoints are not exposed to everyone
Pass	1.2.1	Ensure AWS default Virtual Private Cloud (VPC) is not being used
Fail	1.2.1	Ensure that your EC2 security groups do not allow unrestricted outbound/egress access
Pass	1.2.1	Ensure Application Load Balancer (ALB) with HTTP (Port:80) is not exposed to the public i
Pass	1.2.1	Ensure Application Load Balancer (ALB) with HTTPS (Port:443) is not exposed to the publi
Pass	1.2.1	Ensure Application Load Balancer (ALB) with unencrypted LDAP (TCP:389) is not exposed
Pass	1.2.1	Ensure Application Load Balancer (ALB) with unencrypted Mongo (TCP:27017) is not expo
Pass	1.2.1	Ensure Application Load Balancer (ALB) with service 'NetBios Datagram Service' (TCP:138)
Pass	1.2.1	Ensure Application Load Balancer (ALB) with service 'NetBios Datagram Service' (UDP:138
Pass	1.2.1	Ensure Application Load Balancer (ALB) with service 'NetBIOS Name Service' (TCP:137) is
Pass	1.2.1	Ensure Application Load Balancer (ALB) with service 'NetBIOS Name Service' (UDP:137) is
Pass	1.2.1	Ensure Application Load Balancer (ALB) with service 'NetBios Session Service' (TCP:139) is
Pass	1.2.1	Ensure Application Load Balancer (ALB) with service 'NetBios Session Service' (UDP:139) is
Pass	1.2.1	Ensure Application Load Balancer (ALB) with administrative service: Remote Desktop (TCP
Pass	1.2.1	Ensure Application Load Balancer (ALB) with service 'SNMP' (UDP:161) is not exposed to t
Pass	1.2.1	Ensure Application Load Balancer (ALB) with administrative service: SSH (TCP:22) is not ex
Pass	1.2.1	Ensure Application Load Balancer (ALB) with service 'Prevalent known internal port' (TCP:3

Ensure no Application Load Balancer allows unrestricted inbound access to all UDP traffic

Using AWS Console

1. Sign in to the AWS Management Console.

2. Navigate to EC2 dashboard at https://console.aws.amazon.com/ec2/.

3. In the left navigation panel, under `LOAD BALANCING` section, choose `Load Balancers`

4. In Filter by tags and attribute at the top filter by `Type : Application`

5. Select the Application Load Balancer that you want to reconfigure.

6. Select the `Description` tab from the bottom panel.

7. Under `Security` select source `Security Group`.

8. Select the `Inbound` tab from the dashboard bottom panel and click the Edit button.

9. In the Edit inbound rules dialog box, change the traffic Source for any inbound rules that allow unrestricted access through All UDP port range 0 - 65535 by performing one of the following actions:

- Select My IP from the Source dropdown list to allow inbound traffic only from your machine (from your IP address).
- Select Custom from the Source dropdown list and enter one of the following options based on your access requirements:
  - The static IP/Elastic IP address of the permitted host with the suffix set to /32, e.g. <ip address>/32.
  - The IP address range of the permitted hosts in CIDR notation, for example <ip address>/24.
  - The name or ID of another security group available in the same AWS region.

9. Click `Save` to apply the changes.

10. Repeat steps no. 4 - 10 to update other EC2 security groups that allow unrestricted UDP access, type is All UDP.

11. Change the AWS region from the navigation bar and repeat the process for other regions.

Using AWS CLI

1. Run `describe-load-balancers` using the necessary filters to expose the Application Load Balancers attached to the security groups:

```
aws elbv2 describe-load-balancers --region <region_name> --query "LoadBalancers[?(Type=='application')].SecurityGroups"
```

2. Run `revoke-security-group-ingress` command to remove the inbound rule(s) that allow unrestricted access through All UDP port range 0 - 65535, from the selected EC2 security group (the command does not return an output):

```
aws ec2 revoke-security-group-ingress --region <region-name> --group-id <group id> --ip-permissions "[{\"IpProtocol\": \"UDP\", \"FromPort\": 0 , \"ToPort\": 65535, \"IpRanges\": [{\"CidrIp\": \"0.0.0.0/0\"}]}]"
```

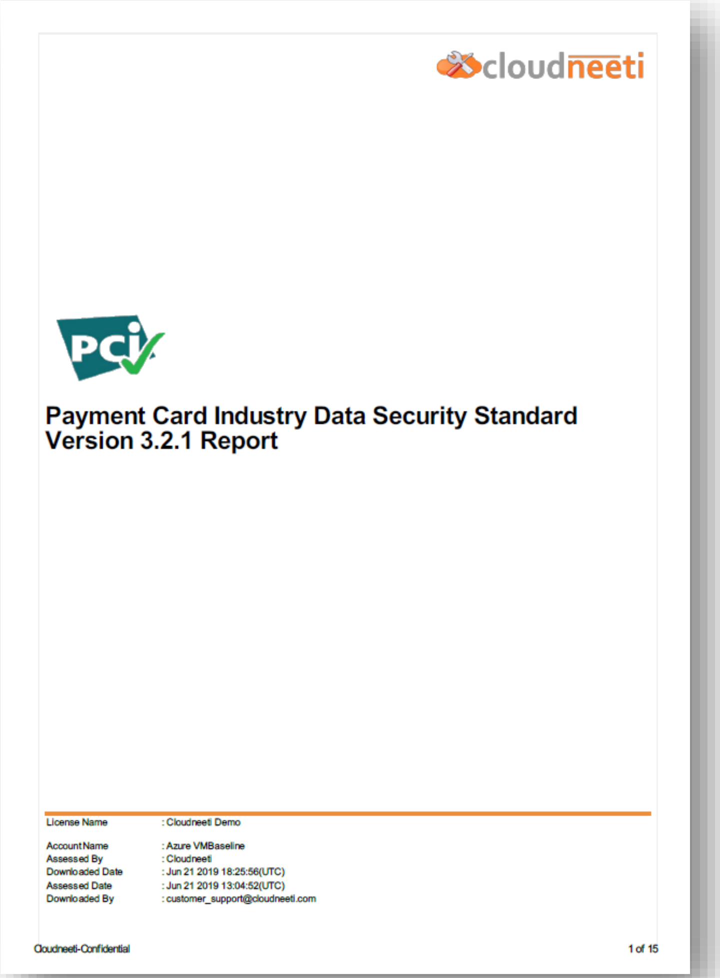
```
aws ec2 revoke-security-group-ingress --region <region-name> --group-id <group id> --ip-permissions "[{\"IpProtocol\": \"UDP\", \"FromPort\": 0 , \"ToPort\": 65535, \"Ipv6Ranges\": [{\"CidrIpv6\": \"::/0\"}]}]"
```

3. Run `authorize-security-group-ingress` command to add the inbound rules removed at the previous step with a different set of parameters in order to restrict type 'All UDP' access to specific entities. To add custom inbound/ingress rules to the selected security group, use one of the following options (the command does not produce an output):

- Add an inbound rule that allows UDP (type All UDP) access to the specific static IP/Elastic IP address of the permitted host

Status	Load Balancer name	Region	Restricted UDP access?
	Filter by Load Balancer name...	Filter by Region...	Filter by Restricted UDP access?...
Pass	poc-app-lb	US East (Ohio)	Yes

Compliance:
1-click downloadable reports for 12+ Security & Compliance Frameworks

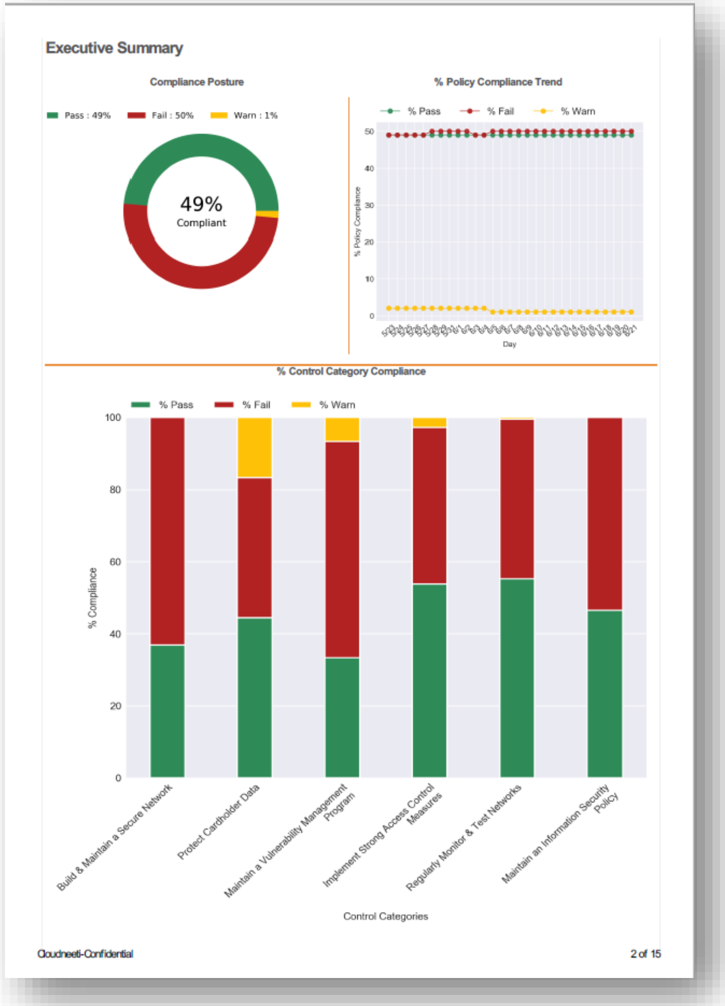


cloudneeti

Payment Card Industry Data Security Standard Version 3.2.1 Report

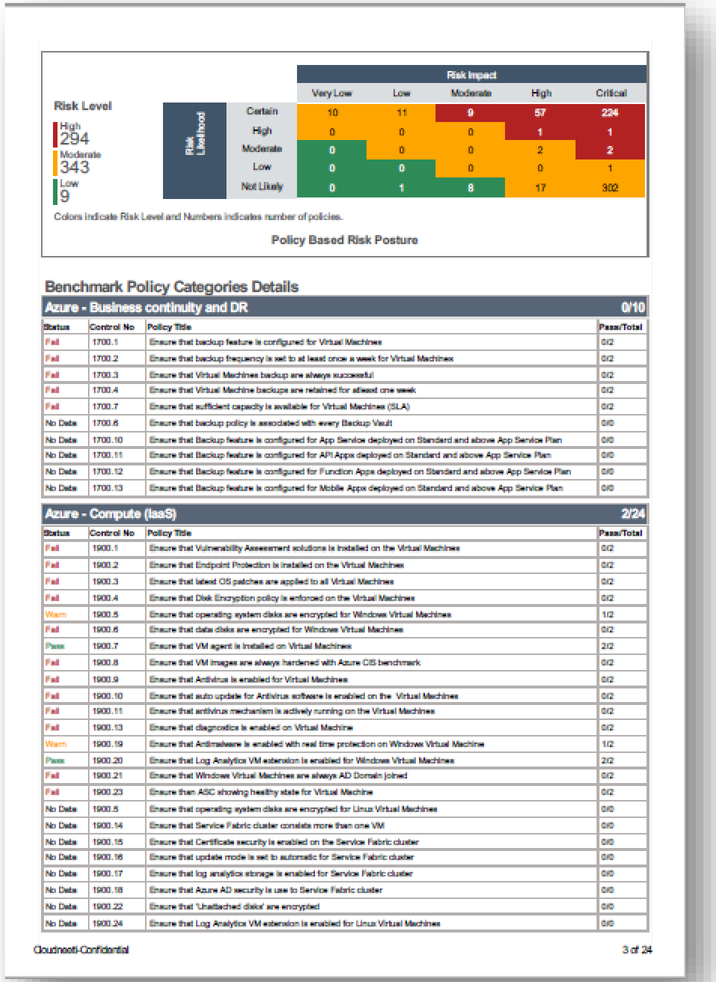
License Name	: Cloudneeti Demo
Account Name	: Azure VMBaseline
Assessed By	: Cloudneeti
Downloaded Date	: Jun 21 2019 18:25:56(UTC)
Assessed Date	: Jun 21 2019 13:04:52(UTC)
Downloaded By	: customer_support@cloudneeti.com

Cloudneeti-Confidential 1 of 15



Executive Summary

Cloudneeti-Confidential 2 of 15



Risk Level

High 294

Moderate 343

Low 9

Risk Likelihood		Risk Impact				
		Very Low	Low	Moderate	High	Critical
	Certain	10	11	9	57	224
	High	0	0	0	1	1
	Moderate	0	0	0	2	2
	Low	0	0	0	0	1
	Not Likely	0	1	8	17	302

Colors indicate Risk Level and Numbers indicates number of policies.

Policy Based Risk Posture

Benchmark Policy Categories Details

Azure - Business continuity and DR 0/10

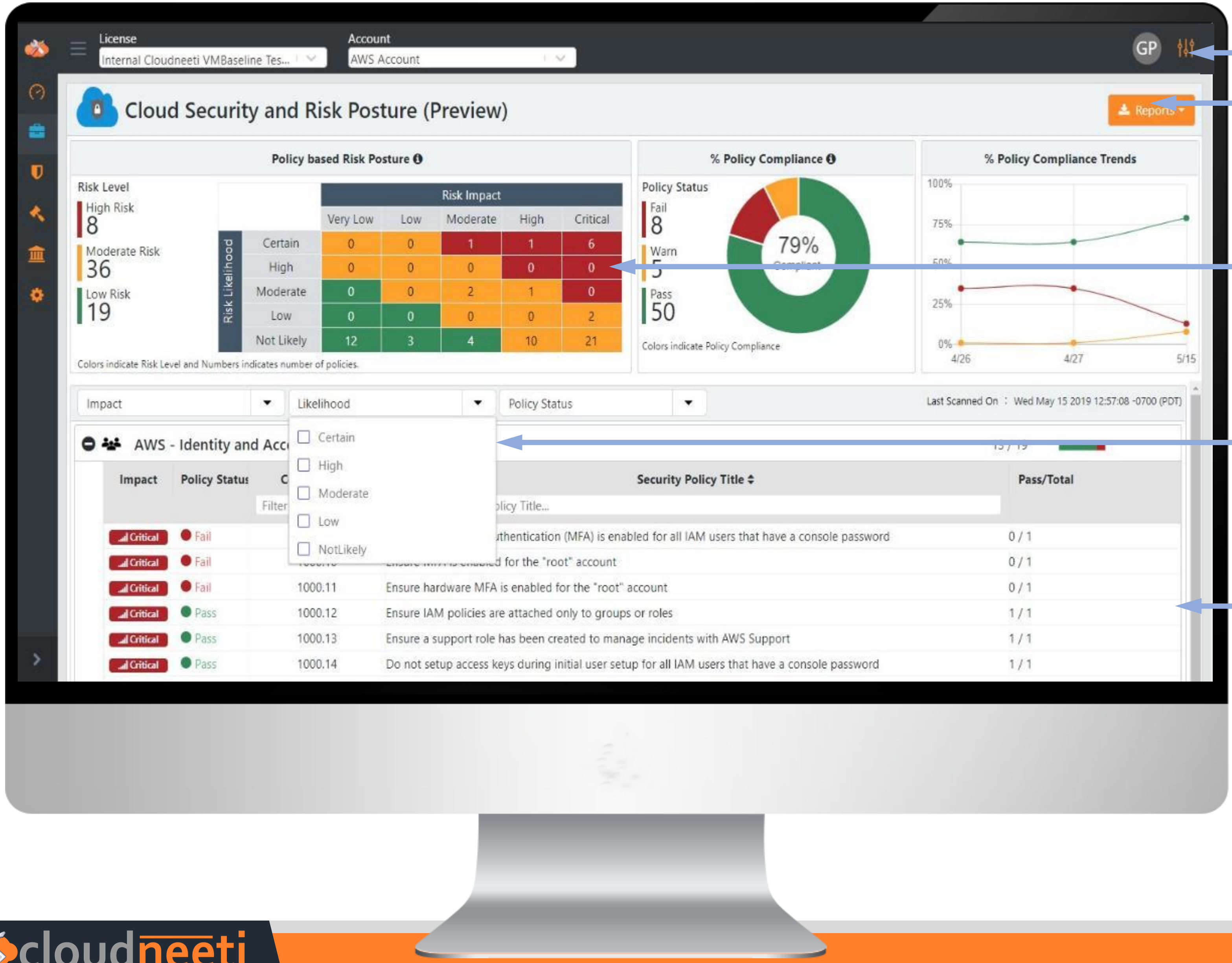
Status	Control No	Policy Title	Pass/Total
Fail	1700.1	Ensure that backup feature is configured for Virtual Machines	0/2
Fail	1700.2	Ensure that backup frequency is set to at least once a week for Virtual Machines	0/2
Fail	1700.3	Ensure that Virtual Machines backup are always successful	0/2
Fail	1700.4	Ensure that Virtual Machine backups are retained for atleast one week	0/2
Fail	1700.7	Ensure that sufficient capacity is available for Virtual Machines (SLA)	0/2
No Data	1700.8	Ensure that backup policy is associated with every Backup Vault	0/0
No Data	1700.10	Ensure that Backup feature is configured for App Service deployed on Standard and above App Service Plan	0/0
No Data	1700.11	Ensure that Backup feature is configured for API Apps deployed on Standard and above App Service Plan	0/0
No Data	1700.12	Ensure that Backup feature is configured for Function Apps deployed on Standard and above App Service Plan	0/0
No Data	1700.13	Ensure that Backup feature is configured for Mobile Apps deployed on Standard and above App Service Plan	0/0

Azure - Compute (IaaS) 2/24

Status	Control No	Policy Title	Pass/Total
Fail	1900.1	Ensure that Vulnerability Assessment solutions is installed on the Virtual Machines	0/2
Fail	1900.2	Ensure that Endpoint Protection is installed on the Virtual Machines	0/2
Fail	1900.3	Ensure that latest OS patches are applied to all Virtual Machines	0/2
Fail	1900.4	Ensure that Disk Encryption policy is enforced on the Virtual Machines	0/2
Warn	1900.5	Ensure that operating system disks are encrypted for Windows Virtual Machines	1/2
Fail	1900.6	Ensure that data disks are encrypted for Windows Virtual Machines	0/2
Pass	1900.7	Ensure that VM agent is installed on Virtual Machines	2/2
Fail	1900.8	Ensure that VM images are always hardened with Azure CIS benchmark	0/2
Fail	1900.9	Ensure that Antivirus is enabled for Virtual Machines	0/2
Fail	1900.10	Ensure that auto update for Antivirus software is enabled on the Virtual Machines	0/2
Fail	1900.11	Ensure that antivirus mechanism is actively running on the Virtual Machines	0/2
Fail	1900.13	Ensure that diagnostics is enabled on Virtual Machine	0/2
Warn	1900.19	Ensure that Antimalware is enabled with real time protection on Windows Virtual Machine	1/2
Pass	1900.20	Ensure that Log Analytics VM extension is enabled for Windows Virtual Machines	2/2
Fail	1900.21	Ensure that Windows Virtual Machines are always AD Domain joined	0/2
Fail	1900.23	Ensure than ASC showing healthy state for Virtual Machine	0/2
No Data	1900.5	Ensure that operating system disks are encrypted for Linux Virtual Machines	0/0
No Data	1900.14	Ensure that Service Fabric cluster consists more than one VM	0/0
No Data	1900.15	Ensure that Certificate security is enabled on the Service Fabric cluster	0/0
No Data	1900.16	Ensure that update mode is set to automatic for Service Fabric cluster	0/0
No Data	1900.17	Ensure that log analytics storage is enabled for Service Fabric cluster	0/0
No Data	1900.18	Ensure that Azure AD security is use to Service Fabric cluster	0/0
No Data	1900.22	Ensure that 'Unattached disks' are encrypted	0/0
No Data	1900.24	Ensure that Log Analytics VM extension is enabled for Linux Virtual Machines	0/0

Cloudneeti-Confidential 3 of 24

Security Posture infused with Risk prioritization allows integrated decision making



License: Internal Cloudneeti VMBaseline Tes...

Account: AWS Account

GP

Cloud Security and Risk Posture (Preview)

Reports

Policy based Risk Posture

Risk Level

- High Risk 8
- Moderate Risk 36
- Low Risk 19

Risk Likelihood	Very Low	Low	Moderate	High	Critical
Certain	0	0	1	1	6
High	0	0	0	0	0
Moderate	0	0	2	1	0
Low	0	0	0	0	2
Not Likely	12	3	4	10	21

Risk Impact

Colors indicate Risk Level and Numbers indicates number of policies.

% Policy Compliance

Policy Status

- Fail 8
- Warn 5
- Pass 50

79% Compliant

Colors indicate Policy Compliance

% Policy Compliance Trends

Impact ▾ | Likelihood ▾ | Policy Status ▾

Last Scanned On : Wed May 15 2019 12:57:08 -0700 (PDT)

Likelihood:
- ☐ Certain
- ☐ High
- ☐ Moderate
- ☐ Low
- ☐ NotLikely

AWS - Identity and Acc

Impact	Policy Status	C	Security Policy Title	Pass/Total
Critical	Fail		thentication (MFA) is enabled for all IAM users that have a console password	0 / 1
Critical	Fail		for the "root" account	0 / 1
Critical	Fail	1000.11	Ensure hardware MFA is enabled for the "root" account	0 / 1
Critical	Pass	1000.12	Ensure IAM policies are attached only to groups or roles	1 / 1
Critical	Pass	1000.13	Ensure a support role has been created to manage incidents with AWS Support	1 / 1
Critical	Pass	1000.14	Do not setup access keys during initial user setup for all IAM users that have a console password	1 / 1

User can request a rescan on demand

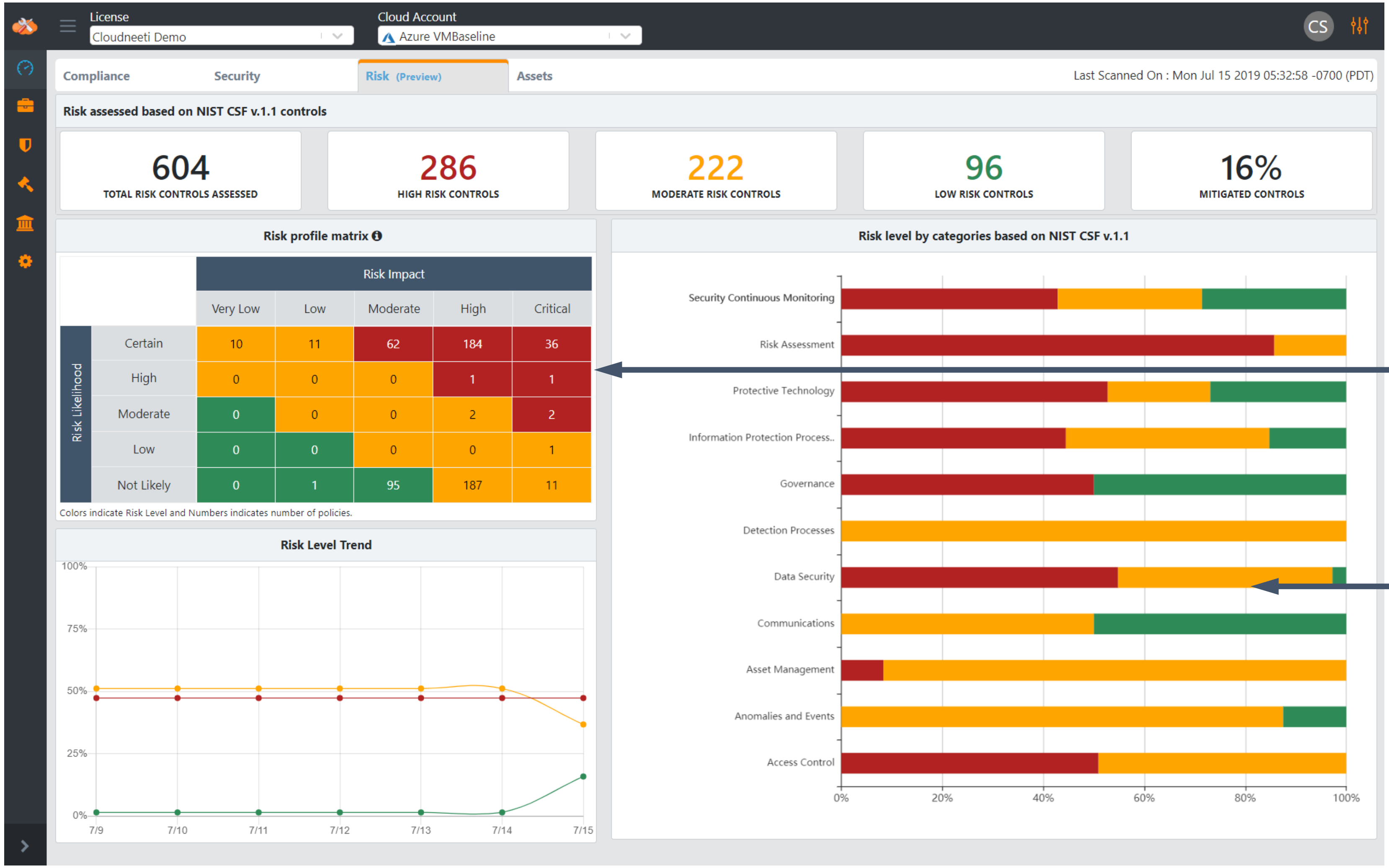
User can generate a PDF report with compliance evidence for auditors

ISO27005/ENISA based Risk Posture dashboard categorizes all misconfigurations by Risk Impact and by Risk Likelihood (rule based Machine Learning). Companies can use this for prioritization of remediations and digital risk management

Filters can be applied to quickly list down policies by impact, likelihood and policy status

Report shows compliance status at an individual security policy level. It displays control number, policy title and number of compliant resources (pass) out of total

Risk: Dashboard provides visibility and prioritization



Last Scanned On : Mon Jul 15 2019 05:32:58 -0700 (PDT)

Risk assessed based on NIST CSF v.1.1 controls

604 TOTAL RISK CONTROLS ASSESSED

286 HIGH RISK CONTROLS

222 MODERATE RISK CONTROLS

96 LOW RISK CONTROLS

16% MITIGATED CONTROLS

Risk profile matrix

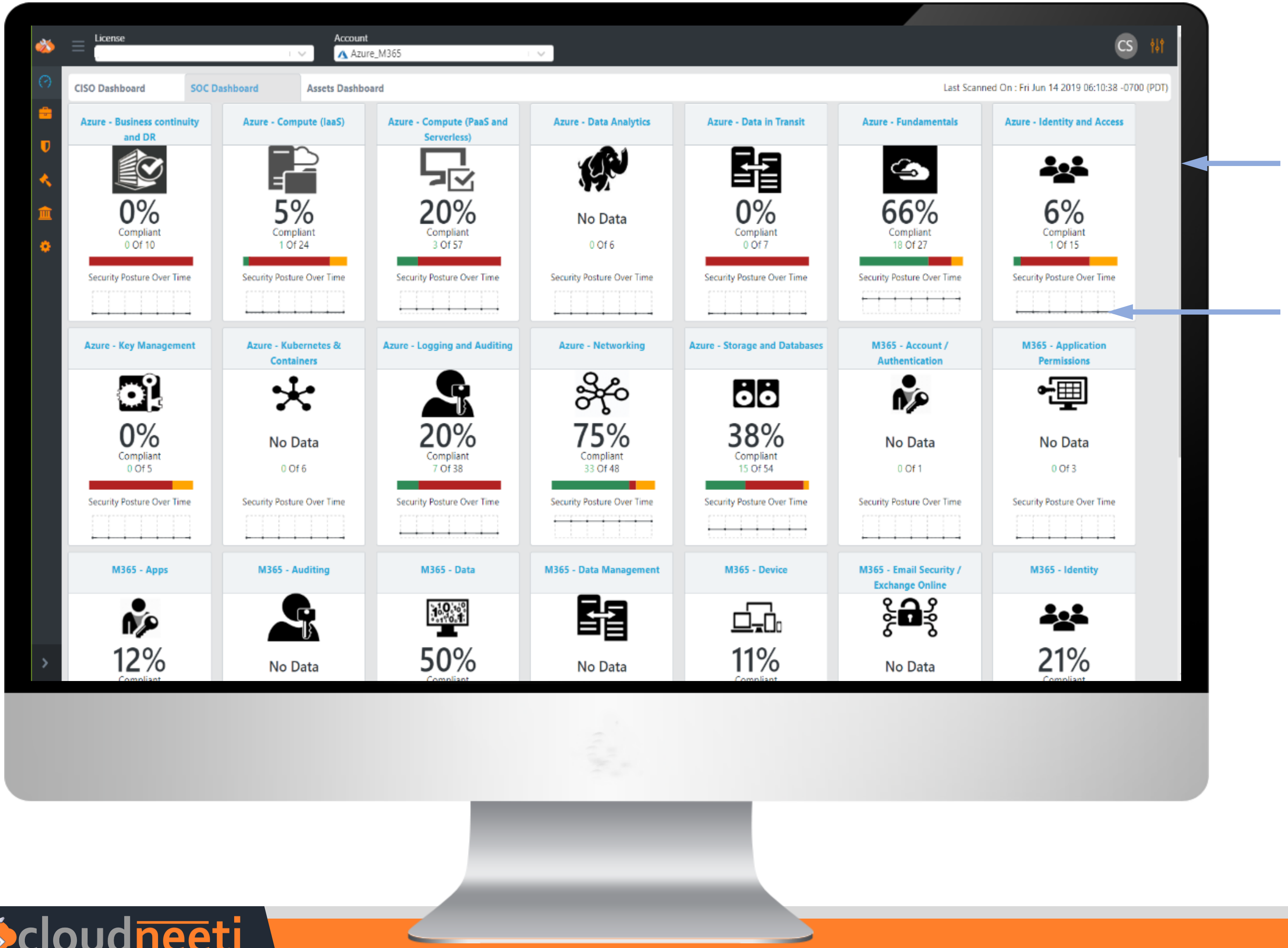
		Risk Impact				
		Very Low	Low	Moderate	High	Critical
Risk Likelihood	Certain	10	11	62	184	36
	High	0	0	0	1	1
	Moderate	0	0	0	2	2
	Low	0	0	0	0	1
	Not Likely	0	1	95	187	11

Colors indicate Risk Level and Numbers indicates number of policies.

ISO27005/ENISA based Risk Posture dashboard categorizes all misconfigurations by Risk Impact and by Risk Likelihood (rule based Machine Learning). Companies can use this for prioritization of remediations and digital risk management

Continuous Assessment using NIST CSF domain categories

SOC Dashboard displays security posture for asset categories



License

Account: Azure_M365

CS

CISO Dashboard | SOC Dashboard | Assets Dashboard

Last Scanned On : Fri Jun 14 2019 06:10:38 -0700 (PDT)

Azure - Business continuity and DR
0%
Compliant
0 Of 10
Security Posture Over Time

Azure - Compute (IaaS)
5%
Compliant
1 Of 24
Security Posture Over Time

Azure - Compute (PaaS and Serverless)
20%
Compliant
3 Of 57
Security Posture Over Time

Azure - Data Analytics
No Data
0 Of 6
Security Posture Over Time

Azure - Data in Transit
0%
Compliant
0 Of 7
Security Posture Over Time

Azure - Fundamentals
66%
Compliant
18 Of 27
Security Posture Over Time

Azure - Identity and Access
6%
Compliant
1 Of 15
Security Posture Over Time

Azure - Key Management
0%
Compliant
0 Of 5
Security Posture Over Time

Azure - Kubernetes & Containers
No Data
0 Of 6
Security Posture Over Time

Azure - Logging and Auditing
20%
Compliant
7 Of 38
Security Posture Over Time

Azure - Networking
75%
Compliant
33 Of 48
Security Posture Over Time

Azure - Storage and Databases
38%
Compliant
15 Of 54
Security Posture Over Time

M365 - Account / Authentication
No Data
0 Of 1
Security Posture Over Time

M365 - Application Permissions
No Data
0 Of 3
Security Posture Over Time

M365 - Apps
12%
Compliant

M365 - Auditing
No Data

M365 - Data
50%
Compliant

M365 - Data Management
No Data

M365 - Device
11%
Compliant

M365 - Email Security / Exchange Online
No Data

M365 - Identity
21%
Compliant

Shows security posture for asset categories

Shows high-level trends over time

Contact Us

Website:
https://www.cloudneeti.com

Documentation:
https://docs.cloudneeti.com

Email:
sales@cloudneeti.com

Contact Us:
https://www.cloudneeti.com/contact_us/