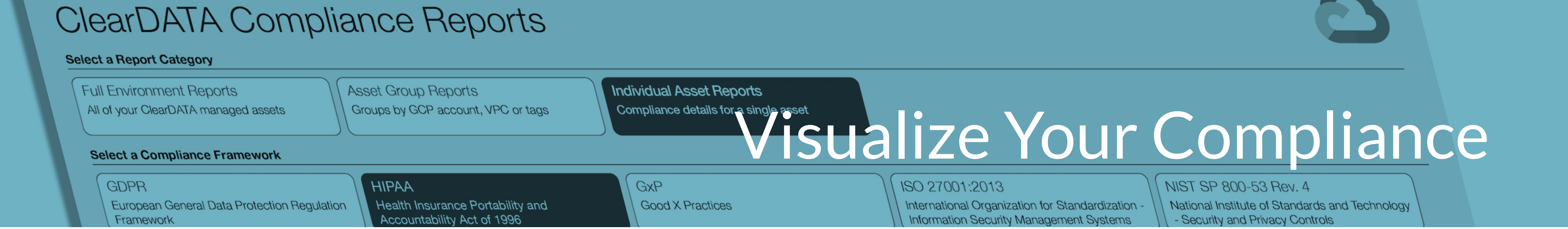

ClearDATA Compliance Reports
Select a Report Category
Full Environment Reports
All of your ClearDATA managed assets
Asset Group Reports
Groups by GCP account, VPC or tags
Individual Asset Reports
Compliance details for a single asset
Select a Compliance Framework
GDPR
European General Data Protection Regulation Framework
HIPAA
Health Insurance Portability and Accountability Act of 1996
GxP
Good X Practices
ISO 27001:2013
International Organization for Standardization - Information Security Management Systems
NIST SP 800-53 Rev. 4
National Institute of Standards and Technology - Security and Privacy Controls

Visualize Your Compliance

Compliance is hard. Standards evolve, new regulations are introduced, and reputational and financial risks only escalate. Before you know it, resources that could otherwise be devoted to patient outcomes, claims management, and the ability to provide innovative solution and research in healthcare and life sciences are being committed to managing compliance posture and gathering artifacts for audits.

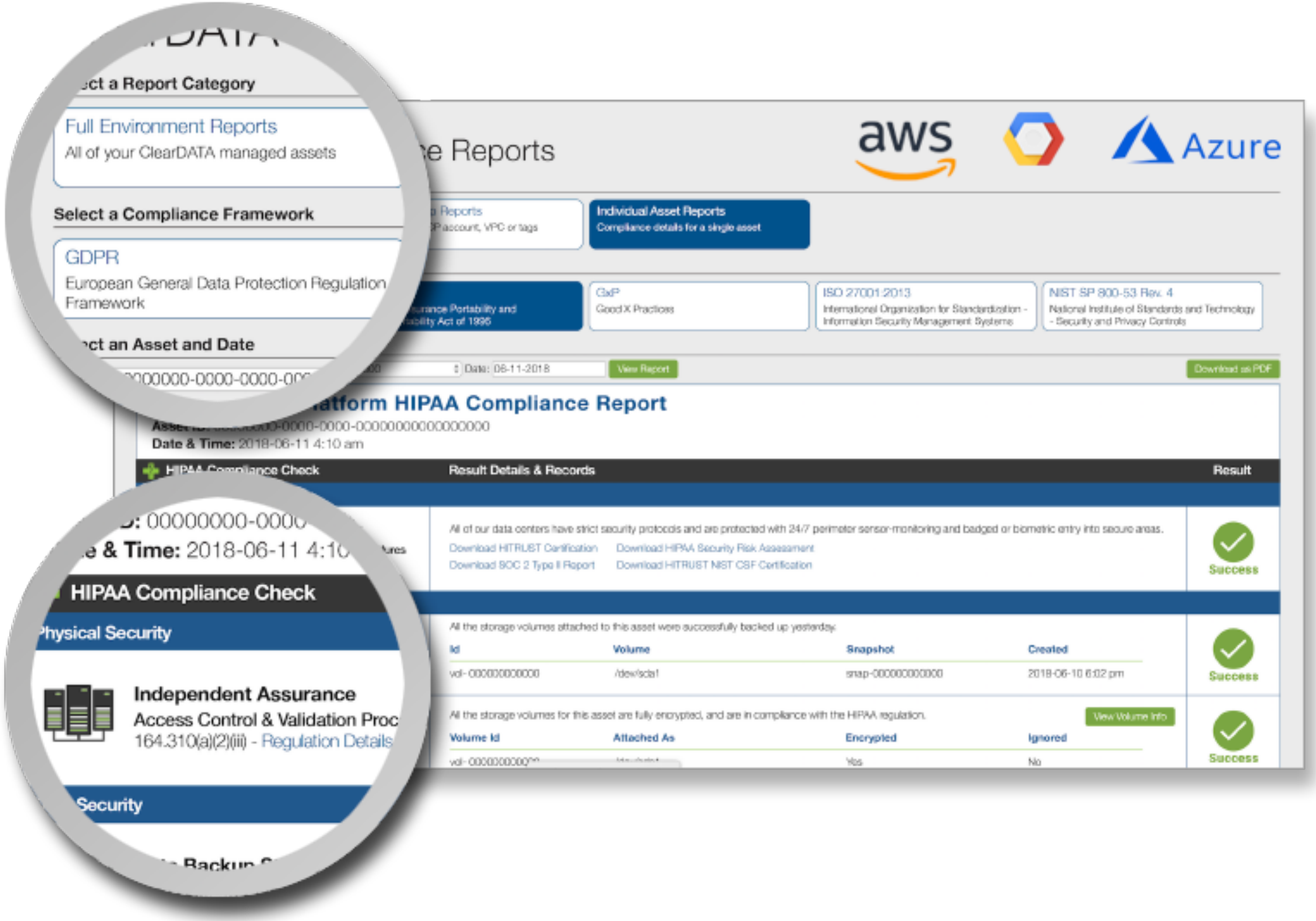
While you might know the necessary controls that need to be put in place, each framework has a different regulation that those controls map to — some referenced as Articles, CFRs, etc. — and, even once you have it mapped out, you still have to figure out what you are going to do to support it so your environment remains compliant.

This is were ClearDATA comes in. We are HITRUST certified experts at security, compliance and privacy in the healthcare cloud. Our managed cloud services include a Compliance Dashboard that gives you a constant view into your environment.

Obtaining visualization and insight into your infrastructure is pivotal to your compliance posture and your ability to assure patients, stakeholders and auditors that you meet or exceed the regulatory standard of each framework you are working within.

Read on to see the difference ClearDATA's Compliance Dashboard can make in improving your ability to focus on your business objectives while we help maintain your compliance.

ClearDATA Compliance Dashboard



DATA

ct a Report Category

Full Environment Reports
All of your ClearDATA managed assets

Select a Compliance Framework

GDPR
European General Data Protection Regulation Framework

ct an Asset and Date

000000-0000-0000-00

e Reports

Reports
P account, VPC or tags

Individual Asset Reports
Compliance details for a single asset

urance Portability and
ability Act of 1996

GxP
Good X Practices

ISO 27001:2013
International Organization for Standardization - Information Security Management Systems

NIST SP 800-53 Rev. 4
National Institute of Standards and Technology - Security and Privacy Controls

Date: 06-11-2018

atform HIPAA Compliance Report

Asset ID: 00000000-0000-0000-0000000000000000
Date & Time: 2018-06-11 4:10 am

D: 00000000-0000
e & Time: 2018-06-11 4:10

HIPAA Compliance Check | Result Details & Records | Result

Physical Security

Independent Assurance
Access Control & Validation Proc
164.310(a)(2)(iii) - Regulation Details

ures

All of our data centers have strict security protocols and are protected with 24/7 perimeter sensor-monitoring and badged or biometric entry into secure areas.

Download HITRUST Certification
Download HIPAA Security Risk Assessment
Download SOC 2 Type II Report
Download HITRUST NIST CSF Certification

Success

Security

Backup

All the storage volumes attached to this asset were successfully backed up yesterday.

Id	Volume	Snapshot	Created
vol- 000000000000	/dev/sda1	snap-000000000000	2018-06-10 6:02 pm

Success

All the storage volumes for this asset are fully encrypted, and are in compliance with the HIPAA regulation.

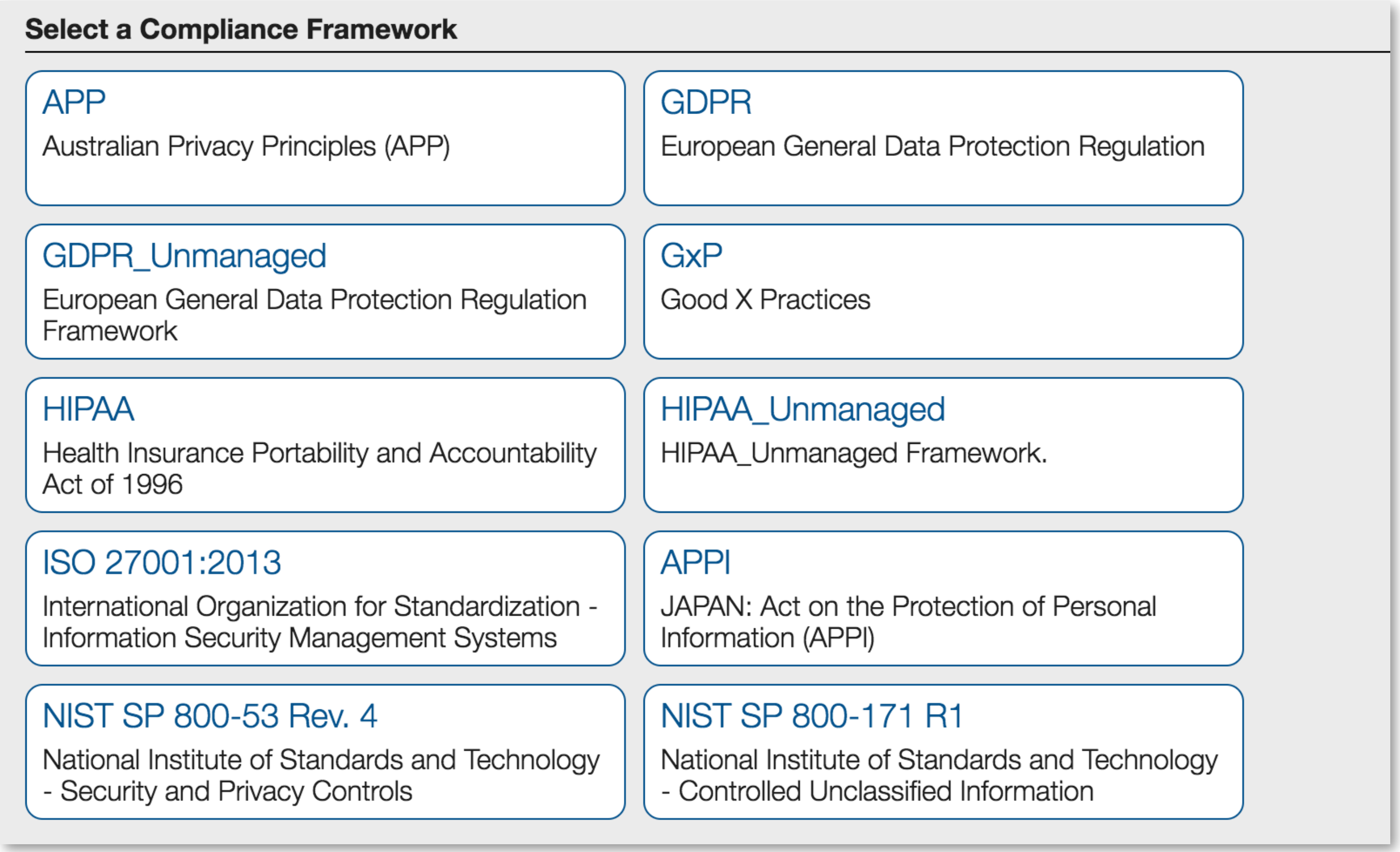
Volume Id	Attached As	Encrypted	Ignored
vol- 00000000000		Yes	No

Success

The ClearDATA Compliance Dashboard gives insight into your data inventory, while also proving the extent to which measures are in place to protect it. It provides you with clear, concise, and auditable views of your cloud environments mapped to multiple compliance disciplines, including:
HIPAA, GDPR, GxP, NIST, ISO 27001.

You can view the compliance status at your full environment level, as a group of assets, or at the individual asset level within AWS, Google Cloud Platform, and/or Azure. On top of that, you can switch between different compliance frameworks and instantly see the results of how your environment, group of assets, or asset stands.

Visualize Your Compliance Status Across Different Standards and Regulations



Select a Compliance Framework

APP
Australian Privacy Principles (APP)

GDPR
European General Data Protection Regulation

GDPR_Unmanaged
European General Data Protection Regulation Framework

GxP
Good X Practices

HIPAA
Health Insurance Portability and Accountability Act of 1996

HIPAA_Unmanaged
HIPAA_Unmanaged Framework.

ISO 27001:2013
International Organization for Standardization - Information Security Management Systems

APPI
JAPAN: Act on the Protection of Personal Information (APPI)

NIST SP 800-53 Rev. 4
National Institute of Standards and Technology - Security and Privacy Controls

NIST SP 800-171 R1
National Institute of Standards and Technology - Controlled Unclassified Information

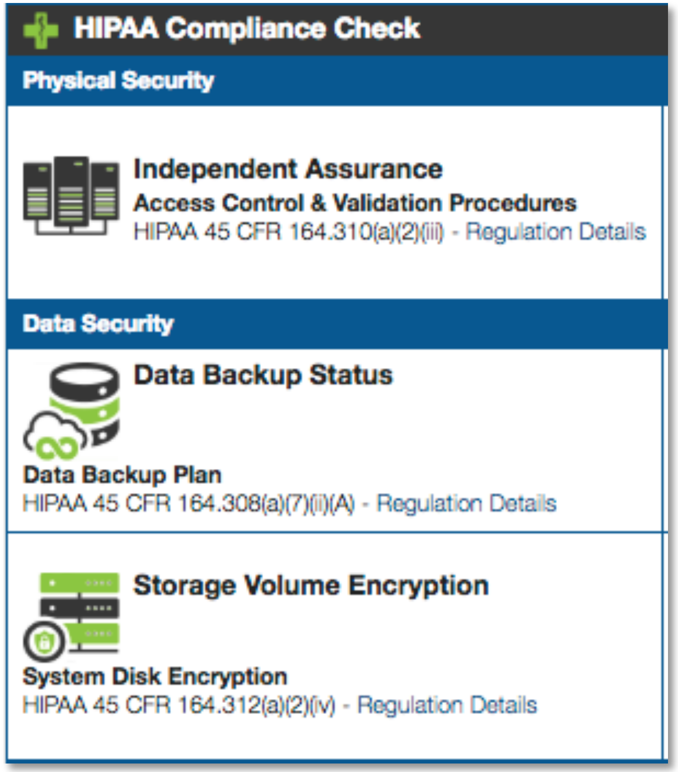
***Figure 1.** In the Compliance Dashboard, you can select from the breadth of supported frameworks and see your compliance status at either an environment level or each individual asset.*

Depending upon the market you sell into or the customers you sell to, your framework adherence might vary.

Rather than having to keep track manually or trust that you and your development team have taken the appropriate actions to secure your environment, now you can instantly see your compliance status across a variety of regulations and standards.

In this dashboard you can switch across different frameworks to see how you comply according to HIPAA, GDPR, or even NIST.

Regulation Mapping to Appropriate IT Controls



HIPAA Compliance Check

Physical Security

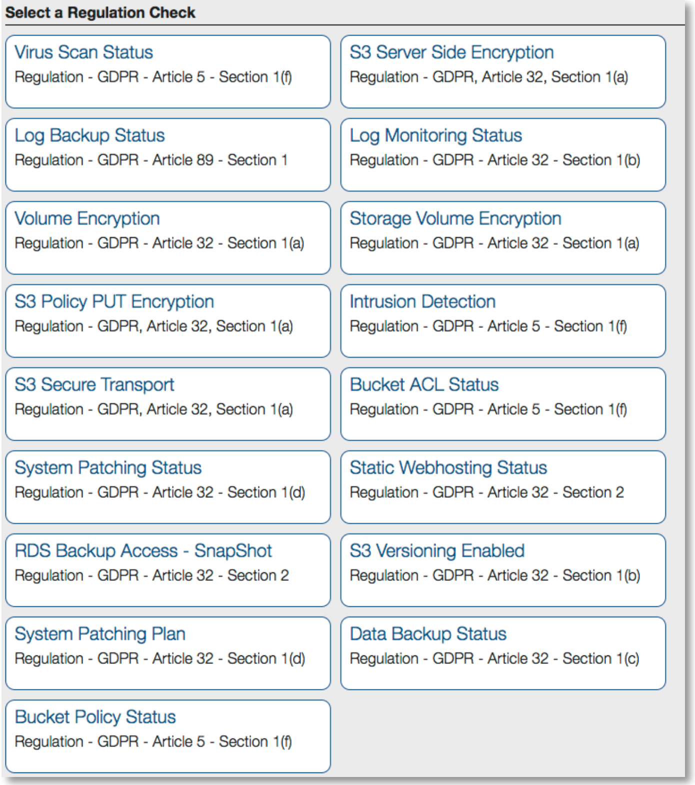
Independent Assurance
Access Control & Validation Procedures
HIPAA 45 CFR 164.310(a)(2)(iii) - Regulation Details

Data Security

Data Backup Status
Data Backup Plan
HIPAA 45 CFR 164.308(a)(7)(ii)(A) - Regulation Details

Storage Volume Encryption
System Disk Encryption
HIPAA 45 CFR 164.312(a)(2)(iv) - Regulation Details

Figure 2. *An example of checks in a the Compliance Dashboard which maps the IT control to the corresponding HIPAA CFR.*



Select a Regulation Check

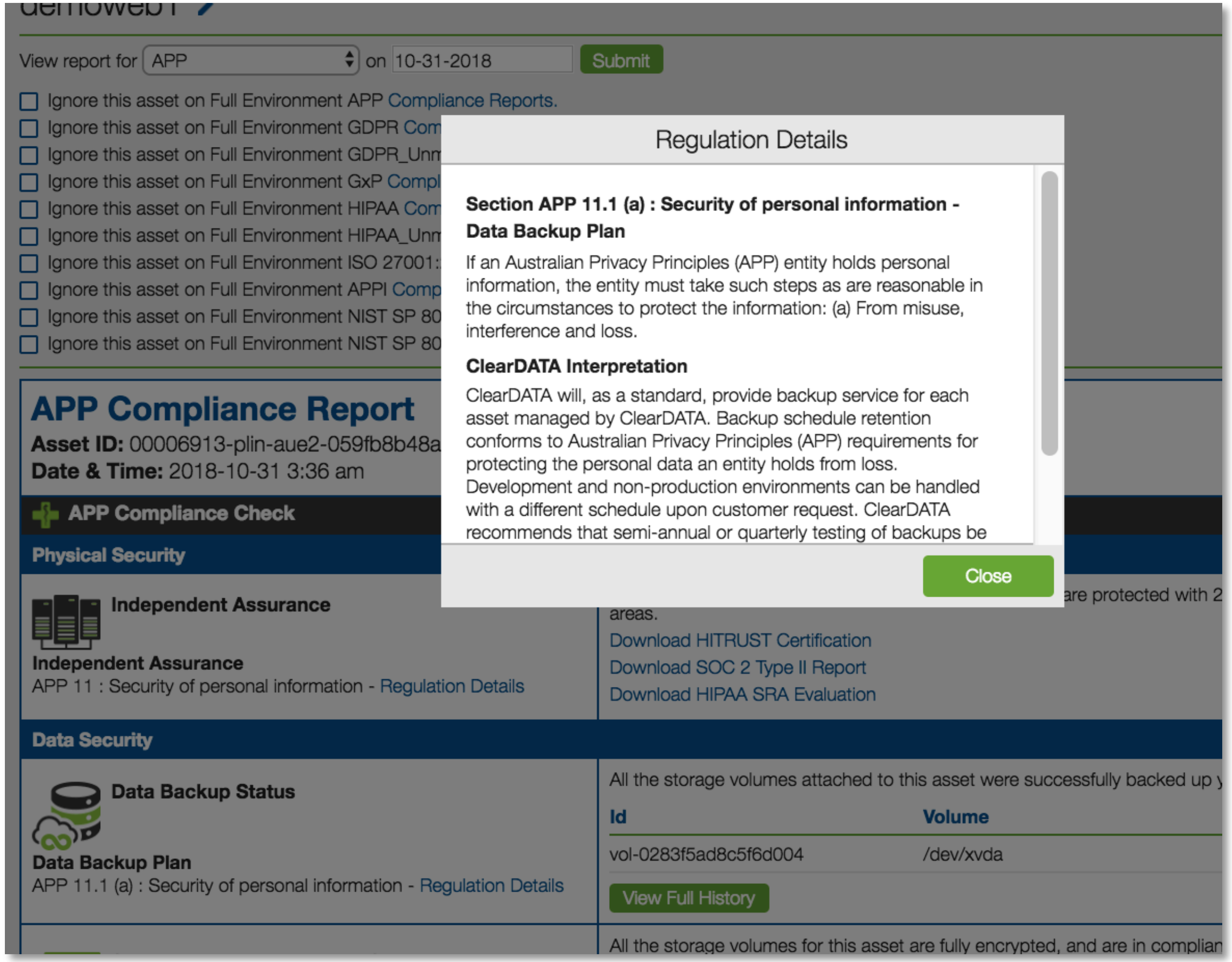
Virus Scan Status Regulation - GDPR - Article 5 - Section 1(f)	S3 Server Side Encryption Regulation - GDPR, Article 32, Section 1(a)
Log Backup Status Regulation - GDPR - Article 89 - Section 1	Log Monitoring Status Regulation - GDPR - Article 32 - Section 1(b)
Volume Encryption Regulation - GDPR - Article 32 - Section 1(a)	Storage Volume Encryption Regulation - GDPR - Article 32 - Section 1(a)
S3 Policy PUT Encryption Regulation - GDPR, Article 32, Section 1(a)	Intrusion Detection Regulation - GDPR - Article 5 - Section 1(f)
S3 Secure Transport Regulation - GDPR, Article 32, Section 1(a)	Bucket ACL Status Regulation - GDPR - Article 5 - Section 1(f)
System Patching Status Regulation - GDPR - Article 32 - Section 1(d)	Static Webhosting Status Regulation - GDPR - Article 32 - Section 2
RDS Backup Access - SnapShot Regulation - GDPR - Article 32 - Section 2	S3 Versioning Enabled Regulation - GDPR - Article 32 - Section 1(b)
System Patching Plan Regulation - GDPR - Article 32 - Section 1(d)	Data Backup Status Regulation - GDPR - Article 32 - Section 1(c)
Bucket Policy Status Regulation - GDPR - Article 5 - Section 1(f)	

Figure 3. *“Checks” like the ones shown above represent the different controls in place mapped to the appropriate regulation. You can select one of the boxes to see your environment status according to one regulation.*

ClearDATA’s Compliance Dashboard can simplify the process of gathering artifacts and demonstrating your organization’s culture of continuous compliance, based upon IT requirements such as virus scans, intrusion detection, logging, back-up, and encryption which are known as “checks” in the dashboard.

Checks connect the necessary IT controls to the appropriate regulation—all visible in the dashboard. Additionally, you can view the status of your full environment according to just one particular regulation, as well as in the overall framework view.

Evidence for an Audit



demoweb1

View report for APP on 10-31-2018 Submit

- □ Ignore this asset on Full Environment APP Compliance Reports.
- □ Ignore this asset on Full Environment GDPR Com
- □ Ignore this asset on Full Environment GDPR_Unm
- □ Ignore this asset on Full Environment GxP Compl
- □ Ignore this asset on Full Environment HIPAA Com
- □ Ignore this asset on Full Environment HIPAA_Unm
- □ Ignore this asset on Full Environment ISO 27001:
- □ Ignore this asset on Full Environment APPI Comp
- □ Ignore this asset on Full Environment NIST SP 80
- □ Ignore this asset on Full Environment NIST SP 80

Regulation Details

Section APP 11.1 (a) : Security of personal information - Data Backup Plan

If an Australian Privacy Principles (APP) entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information: (a) From misuse, interference and loss.

ClearDATA Interpretation

ClearDATA will, as a standard, provide backup service for each asset managed by ClearDATA. Backup schedule retention conforms to Australian Privacy Principles (APP) requirements for protecting the personal data an entity holds from loss. Development and non-production environments can be handled with a different schedule upon customer request. ClearDATA recommends that semi-annual or quarterly testing of backups be

Close

APP Compliance Report

Asset ID: 00006913-plin-aue2-059fb8b48a

Date & Time: 2018-10-31 3:36 am

APP Compliance Check

Physical Security

Independent Assurance

Independent Assurance
APP 11 : Security of personal information - Regulation Details

are protected with 2 areas.

Download HITRUST Certification
Download SOC 2 Type II Report
Download HIPAA SRA Evaluation

Data Security

Data Backup Status

Data Backup Plan
APP 11.1 (a) : Security of personal information - Regulation Details

All the storage volumes attached to this asset were successfully backed up y

Id	Volume
vol-0283f5ad8c5f6d004	/dev/xvda

View Full History

All the storage volumes for this asset are fully encrypted, and are in complian

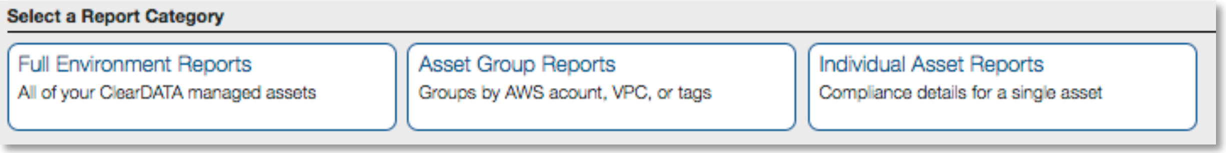
Figure 4. *The Regulation Details are available for every check and provide documentation around the particular regulation. The ClearDATA interpretation describes the controls in place in the cloud.*

It's not just about pass or fail. As many healthcare and life sciences companies know, audits are a regularly occurring event that keep organizations true and disciplined. But at the same time, a lot of work is required to gather all of the evidence needed to prepare for the audit.

After all, it's not enough to say you are compliant, you must prove it. Within the Compliance Dashboard, you can see the language of the regulation and the ClearDATA interpretation.

This documents how the regulation is being met, and when security and compliance questions arise, this view can be easily shared with leadership, auditors and your customers.

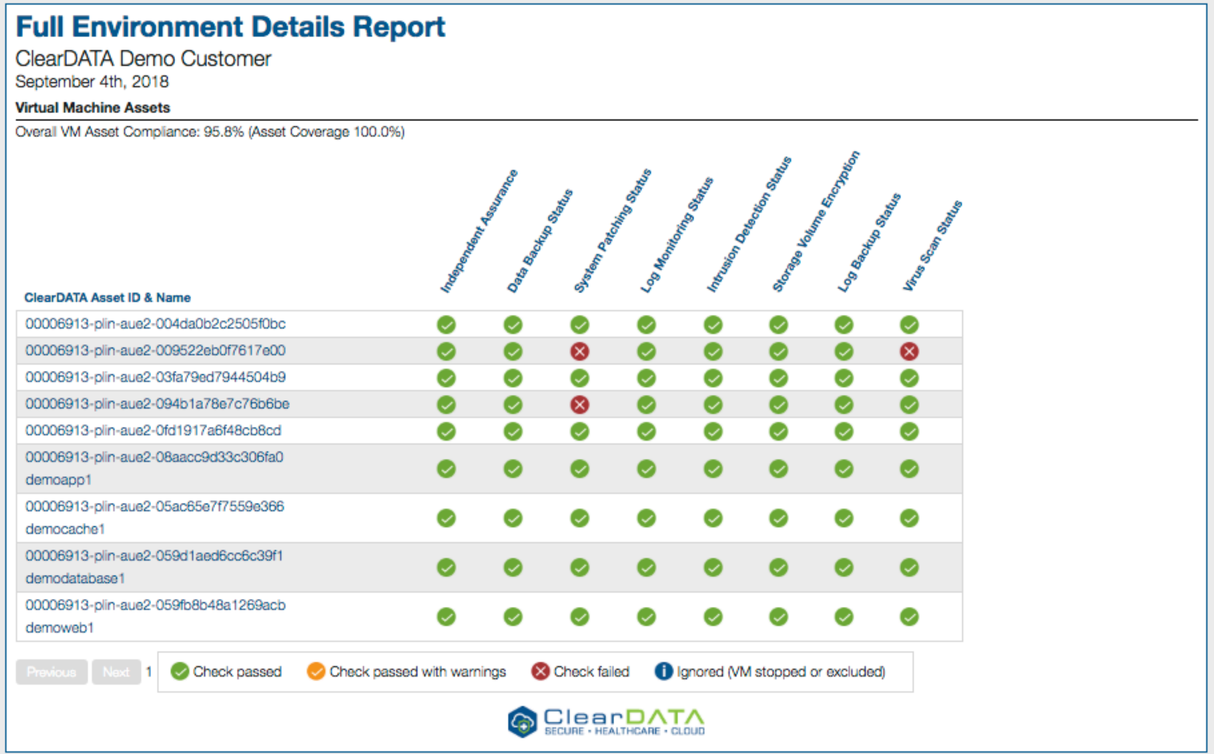
Understand Your Compliance Status at any Level



Select a Report Category

Full Environment Reports	Asset Group Reports	Individual Asset Reports
All of your ClearDATA managed assets	Groups by AWS acount, VPC, or tags	Compliance details for a single asset

***Figure 5**. Select from different levels of detail to view your compliance status.*



Full Environment Details Report

ClearDATA Demo Customer

September 4th, 2018

Virtual Machine Assets

Overall VM Asset Compliance: 95.8% (Asset Coverage 100.0%)

ClearDATA Asset ID & Name	Independent Assurance	Data Backup Status	System Patching Status	Log Monitoring Status	Intrusion Detection Status	Storage Volume Encryption	Log Backup Status	Virus Scan Status
00006913-plin-aue2-004da0b2c2505f0bc	✓	✓	✓	✓	✓	✓	✓	✓
00006913-plin-aue2-009522eb0f7617e00	✓	✓	☒	✓	✓	✓	✓	☒
00006913-plin-aue2-03fa79ed7944504b9	✓	✓	✓	✓	✓	✓	✓	✓
00006913-plin-aue2-094b1a78e7c76b6be	✓	✓	☒	✓	✓	✓	✓	✓
00006913-plin-aue2-0fd1917a6f48cb8cd	✓	✓	✓	✓	✓	✓	✓	✓
00006913-plin-aue2-08aacc9d33c306fa0 demoapp1	✓	✓	✓	✓	✓	✓	✓	✓
00006913-plin-aue2-05ac65e7f7559e366 democache1	✓	✓	✓	✓	✓	✓	✓	✓
00006913-plin-aue2-059d1aed6cc6c39f1 demodatabase1	✓	✓	✓	✓	✓	✓	✓	✓
00006913-plin-aue2-059fb8b48a1269acb demoweb1	✓	✓	✓	✓	✓	✓	✓	✓

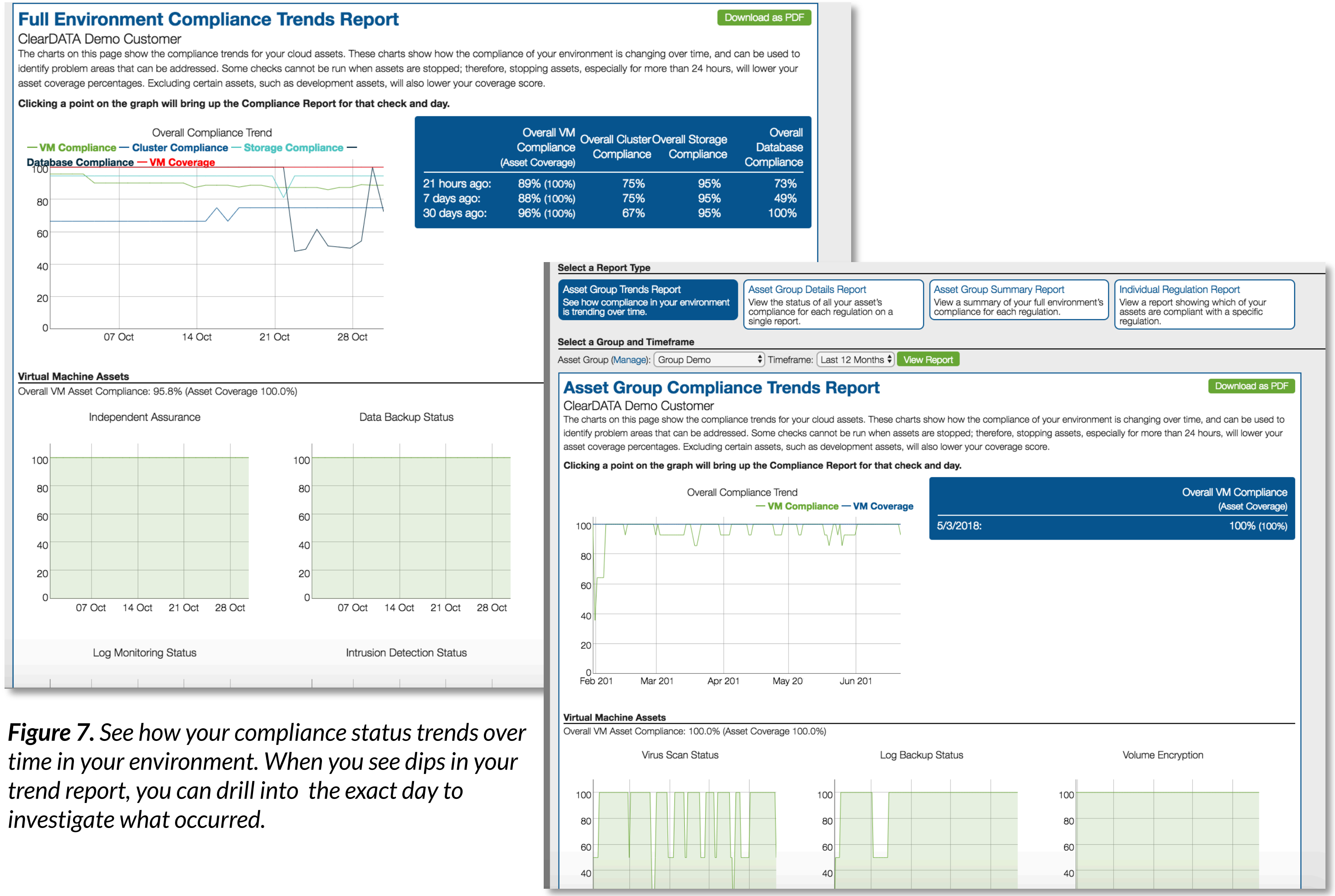
✓ Check passed ● Check passed with warnings ☒ Check failed ⓘ Ignored (VM stopped or excluded)

***Figure 6.** The Full Environment Details Report provides a status of all of the assets' compliance for each regulation on a single report*

Current scorecards and historical trending data by cloud service, regulatory framework, or geographic region make it easy to view your attainment of compliance objectives over time. Assets can also be easily grouped to represent a given application, team, or line of business.

This lets you separate and see compliance on a per project basis, especially as many projects might have different frameworks they must adhere to based upon the location of the data. This also lets you decouple your sandbox environments from your production environments so that you can monitor compliance status for only the environments that require it.

See Your Compliance Status Over Time



Full Environment Compliance Trends Report

ClearDATA Demo Customer

The charts on this page show the compliance trends for your cloud assets. These charts show how the compliance of your environment is changing over time, and can be used to identify problem areas that can be addressed. Some checks cannot be run when assets are stopped; therefore, stopping assets, especially for more than 24 hours, will lower your asset coverage percentages. Excluding certain assets, such as development assets, will also lower your coverage score.

Clicking a point on the graph will bring up the Compliance Report for that check and day.

	Overall VM Compliance (Asset Coverage)	Overall Cluster Compliance	Overall Storage Compliance	Overall Database Compliance
21 hours ago:	89% (100%)	75%	95%	73%
7 days ago:	88% (100%)	75%	95%	49%
30 days ago:	96% (100%)	67%	95%	100%

Virtual Machine Assets

Overall VM Asset Compliance: 95.8% (Asset Coverage 100.0%)

Select a Report Type

Asset Group Trends Report: See how compliance in your environment is trending over time.

Asset Group Details Report: View the status of all your asset's compliance for each regulation on a single report.

Asset Group Summary Report: View a summary of your full environment's compliance for each regulation.

Individual Regulation Report: View a report showing which of your assets are compliant with a specific regulation.

Select a Group and Timeframe

Asset Group (Manage): Group Demo Timeframe: Last 12 Months

Asset Group Compliance Trends Report

ClearDATA Demo Customer

The charts on this page show the compliance trends for your cloud assets. These charts show how the compliance of your environment is changing over time, and can be used to identify problem areas that can be addressed. Some checks cannot be run when assets are stopped; therefore, stopping assets, especially for more than 24 hours, will lower your asset coverage percentages. Excluding certain assets, such as development assets, will also lower your coverage score.

Clicking a point on the graph will bring up the Compliance Report for that check and day.

	Overall VM Compliance (Asset Coverage)
5/3/2018:	100% (100%)

Virtual Machine Assets

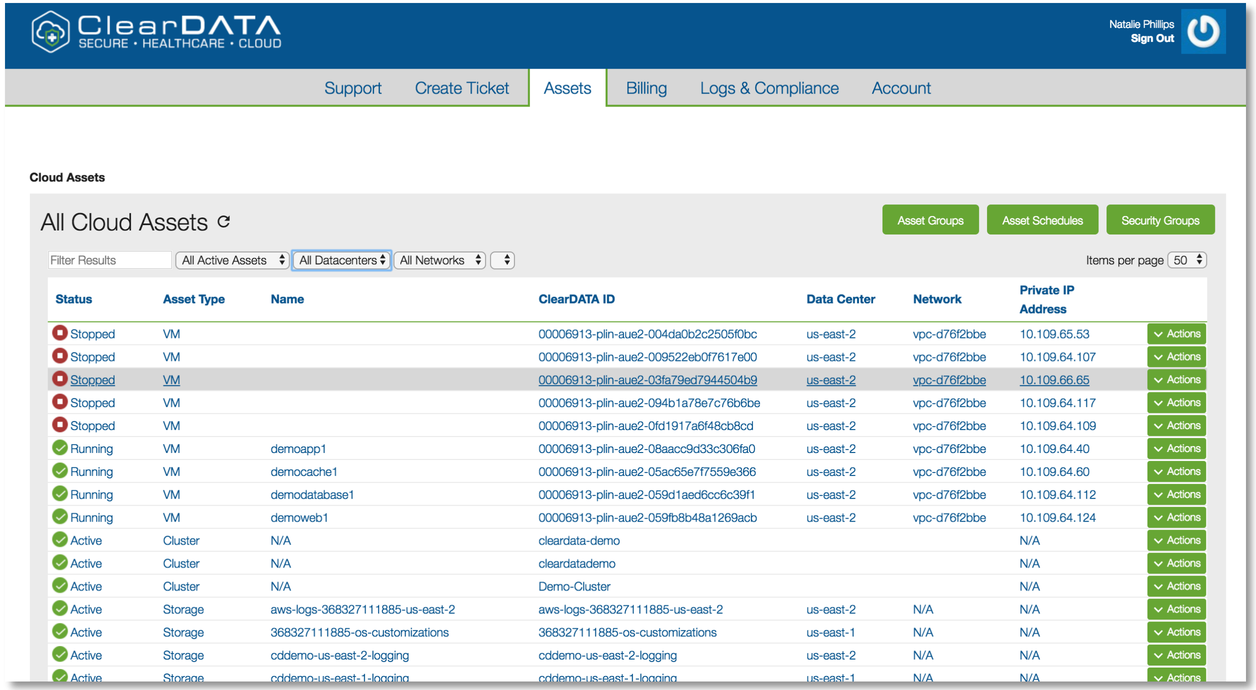
Overall VM Asset Compliance: 100.0% (Asset Coverage 100.0%)

Figure 7. *See how your compliance status trends over time in your environment. When you see dips in your trend report, you can drill into the exact day to investigate what occurred.*

See trends of your full environment over a timeframe – 30 days, 90 days, six months, or a year – and see overall compliance of your assets as it relates to a certain check such as vulnerability scan or log backup.

ClearDATA collects all of the Operating System audit logs and makes them available through the portal. Logs are retained for six years and always available for download.

View Your Data Inventory



Status	Asset Type	Name	ClearDATA ID	Data Center	Network	Private IP Address	
Stopped	VM		00006913-plin-aue2-004da0b2c2505f0bc	us-east-2	vpc-d76f2bbe	10.109.65.53	Actions
Stopped	VM		00006913-plin-aue2-009522eb0f7617e00	us-east-2	vpc-d76f2bbe	10.109.64.107	Actions
Stopped	VM		00006913-plin-aue2-03fa79ed7944504b9	us-east-2	vpc-d76f2bbe	10.109.66.65	Actions
Stopped	VM		00006913-plin-aue2-094b1a78e7c76b6be	us-east-2	vpc-d76f2bbe	10.109.64.117	Actions
Stopped	VM		00006913-plin-aue2-0fd1917a6f48cb8cd	us-east-2	vpc-d76f2bbe	10.109.64.109	Actions
Running	VM	demoapp1	00006913-plin-aue2-08aacc9d33c306fa0	us-east-2	vpc-d76f2bbe	10.109.64.40	Actions
Running	VM	democache1	00006913-plin-aue2-05ac65e7f7559e366	us-east-2	vpc-d76f2bbe	10.109.64.60	Actions
Running	VM	demodatabase1	00006913-plin-aue2-059d1aed6cc6c39f1	us-east-2	vpc-d76f2bbe	10.109.64.112	Actions
Running	VM	demoweb1	00006913-plin-aue2-059fb8b48a1269acb	us-east-2	vpc-d76f2bbe	10.109.64.124	Actions
Active	Cluster	N/A	cleardata-demo			N/A	Actions
Active	Cluster	N/A	cleardatademo			N/A	Actions
Active	Cluster	N/A	Demo-Cluster			N/A	Actions
Active	Storage	aws-logs-368327111885-us-east-2	aws-logs-368327111885-us-east-2	us-east-2	N/A	N/A	Actions
Active	Storage	368327111885-os-customizations	368327111885-os-customizations	us-east-1	N/A	N/A	Actions
Active	Storage	cddemo-us-east-2-logging	cddemo-us-east-2-logging	us-east-2	N/A	N/A	Actions
Active	Storage	cddemo-us-east-1-logging	cddemo-us-east-1-logging	us-east-1	N/A	N/A	Actions

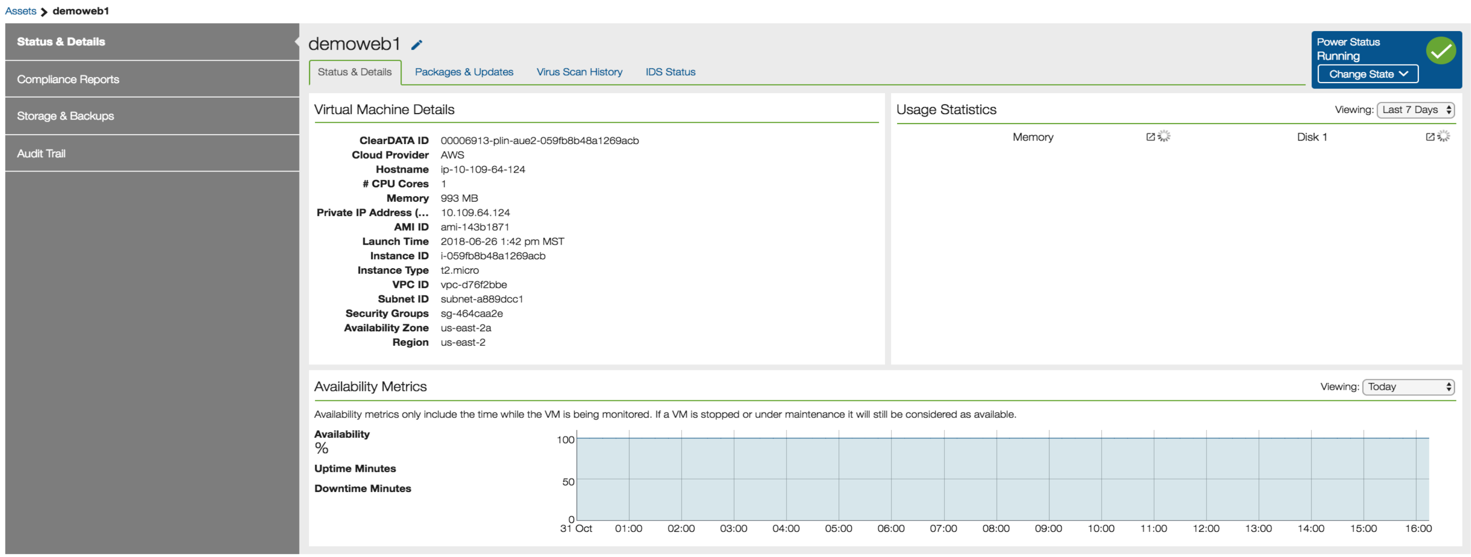
***Figure 8.** The Asset tab within the Compliance Dashboard allows you to drill down to gather more details around your assets.*

Within healthcare IT, it's imperative to know where your data lives. HIPAA and GDPR require it. Security Risk Assessments typically start with looking at an organization's PHI inventory, which often, doesn't exist.

The Compliance Dashboard provides an inventory of your cloud environment—down to the individual asset level. Rather than pulling individual services within your cloud console, the dashboard provides a snapshot view of all cloud resources currently in-use, which provides:

- An asset inventory of all of your compute clusters
- An inventory of all of your assets within each of the different cloud services
- A way to drill down into a specific asset and see details such as the instance type and availability zone
- A view of the results of scheduled scans for Anti-Virus
- A visual history of the IDS agents communication with the IDS monitoring appliance

Understand Your Individual Assets



Virtual Machine Details

ClearDATA ID	00006913-plin-aue2-059fb8b48a1269acb
Cloud Provider	AWS
Hostname	ip-10-109-64-124
# CPU Cores	1
Memory	993 MB
Private IP Address (...	10.109.64.124
AMI ID	ami-143b1871
Launch Time	2018-06-26 1:42 pm MST
Instance ID	i-059fb8b48a1269acb
Instance Type	t2.micro
VPC ID	vpc-d76f2bbe
Subnet ID	subnet-a889dcc1
Security Groups	sg-464caa2e
Availability Zone	us-east-2a
Region	us-east-2

Availability metrics only include the time while the VM is being monitored. If a VM is stopped or under maintenance it will still be considered as available.

Availability %

Uptime Minutes

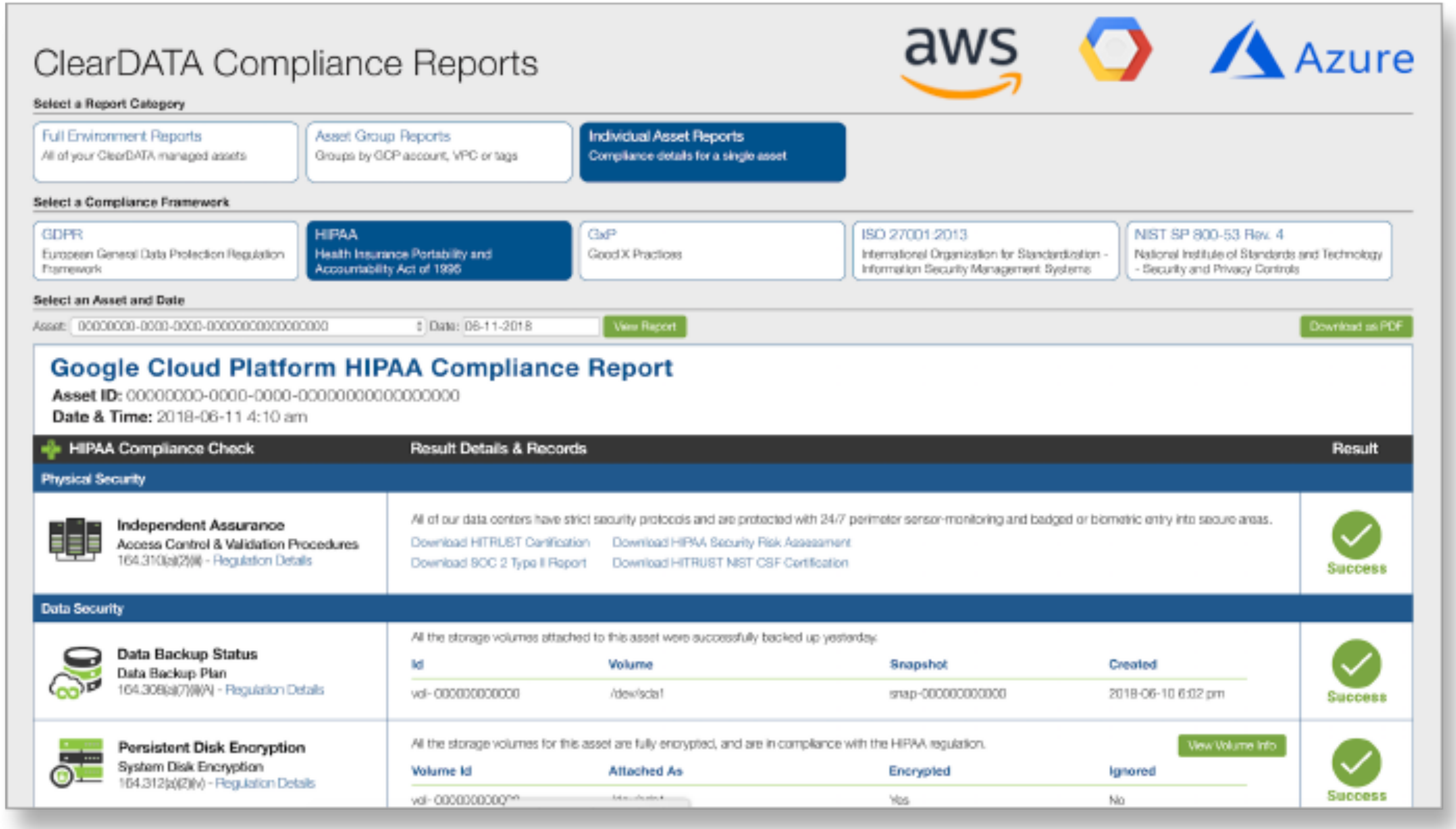
Downtime Minutes

Figure 9. *A compliance report at the individual asset level.*

In addition to understanding your entire environment, you can drill down to gain details about your individual assets such as:

- Instance type and regions
- Usage statistics for memory and disk on the machine
- Available security updates
- Communication history of IDS agents with IDS monitoring appliance
- Volume type, if the volume is encrypted, and the size of the volume
- Snapshot history along with the snapshot ID and the related volume for the snapshot
- Compliance status at the asset level
- All packages installed on the machine and available updates
- Scheduled Anti-Virus scans for the server and the latest definitions the AV agent uses
- Audit trail for the user accounts and virtual machine logins
- Downloadable log entry, including logs older than 45 days

Learn more about the Compliance Dashboard



ClearDATA Compliance Reports

Select a Report Category

- Full Environment Reports — All of your ClearDATA managed assets
- Asset Group Reports — Groups by GCP account, VPC or tags
- Individual Asset Reports — Compliance details for a single asset

Select a Compliance Framework

- GDPR — European General Data Protection Regulation Framework
- HIPAA — Health Insurance Portability and Accountability Act of 1996
- GxP — Good X Practices
- ISO 27001:2013 — International Organization for Standardization - Information Security Management Systems
- NIST SP 800-53 Rev. 4 — National Institute of Standards and Technology - Security and Privacy Controls

Select an Asset and Date

Asset: 00000000-0000-0000-0000000000000000 Date: 06-11-2018 View Report Download as PDF

Google Cloud Platform HIPAA Compliance Report

Asset ID: 00000000-0000-0000-0000000000000000
Date & Time: 2018-06-11 4:10 am

HIPAA Compliance Check	Result Details & Records	Result
Physical Security		
Independent Assurance Access Control & Validation Procedures 164.310(a)(2)(ii) - Regulation Details	All of our data centers have strict security protocols and are protected with 24/7 perimeter sensor-monitoring and badged or biometric entry into secure areas. Download HITRUST Certification Download HIPAA Security Risk Assessment Download SOC 2 Type II Report Download HITRUST NIST CSF Certification	✓ Success
Data Security		
Data Backup Status Data Backup Plan 164.308(a)(7)(ii)(A) - Regulation Details	All the storage volumes attached to this asset were successfully backed up yesterday. Id / Volume / Snapshot / Created vol-000000000000 / /dev/sda1 / snap-000000000000 / 2018-06-10 6:02 pm	✓ Success
Persistent Disk Encryption System Disk Encryption 164.312(a)(2)(iv) - Regulation Details	All the storage volumes for this asset are fully encrypted, and are in compliance with the HIPAA regulation. View Volume Info Volume Id / Attached As / Encrypted / Ignored vol-000000000000 / /dev/sda1 / Yes / No	✓ Success

Don’t let compliance get in the way of your innovation in the cloud — visualize your compliance in AWS, Azure, and Google Cloud Platform with ClearDATA’s Compliance Dashboard.

Learn More:

https://www.cleardata.com/solutions/compliance/