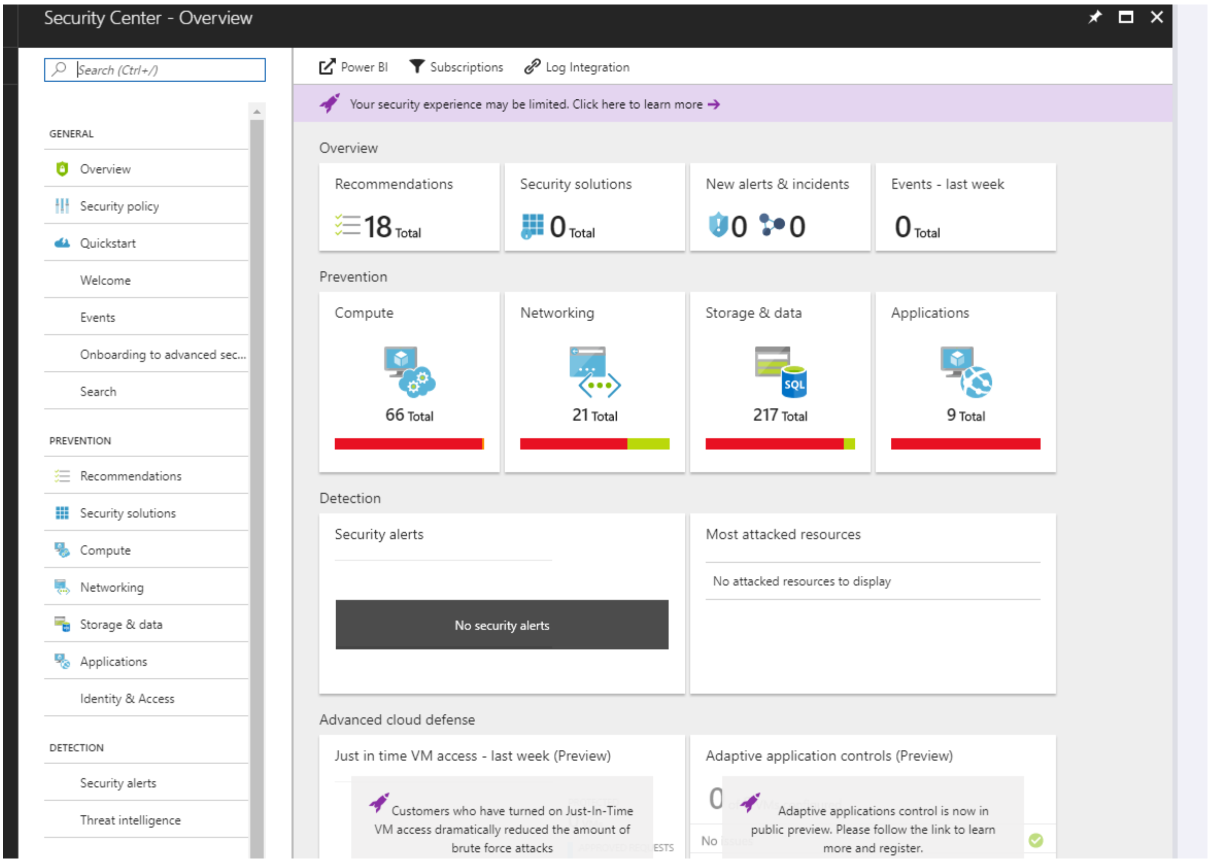
Cybersecurity in Azure

Azure Security Centre:

Azure has its own security centre - a built-in tool that can help prevent, detect, and respond to threats quickly as soon as they arise.

The Azure Security Centre can be accessed through the main menu of the Azure Portal.

When you open the security centre dashboard, you are faced with the ‘Overview’, a summary of the status of your subscriptions, their level of protection, and any recommendations that the security centre might have, in order to tighten security in your cloud network.



Your security experience may be limited. Click here to learn more →

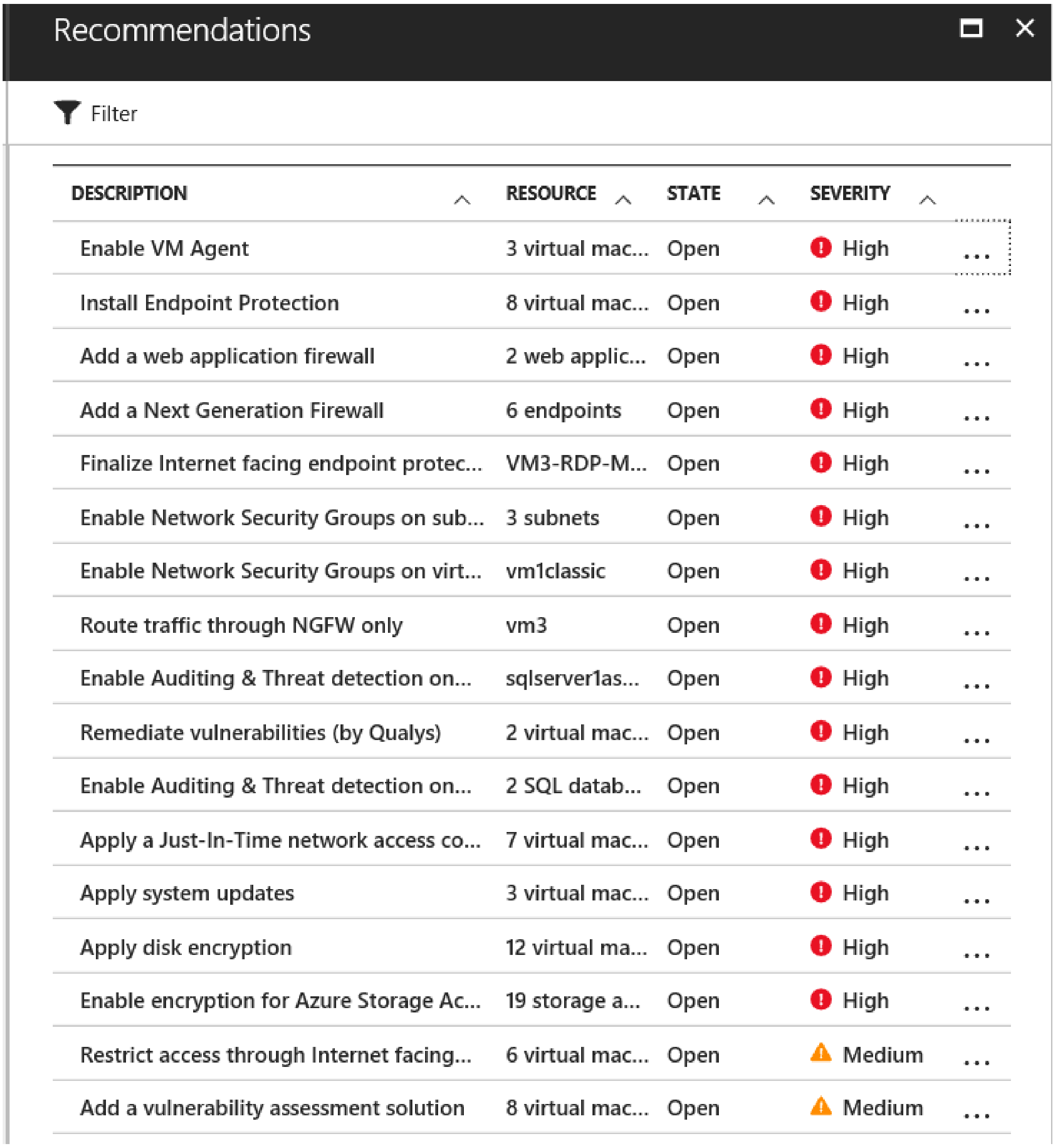
No attacked resources to display

Customers who have turned on Just-In-Time VM access dramatically reduced the amount of brute force attacks

Adaptive applications control is now in public preview. Please follow the link to learn more and register.

CONFIGURE

Clicking the ‘Recommendations’ tile will list them in a new blade, and you can select each one to view more information about each recommendation and take steps to resolve any issues.



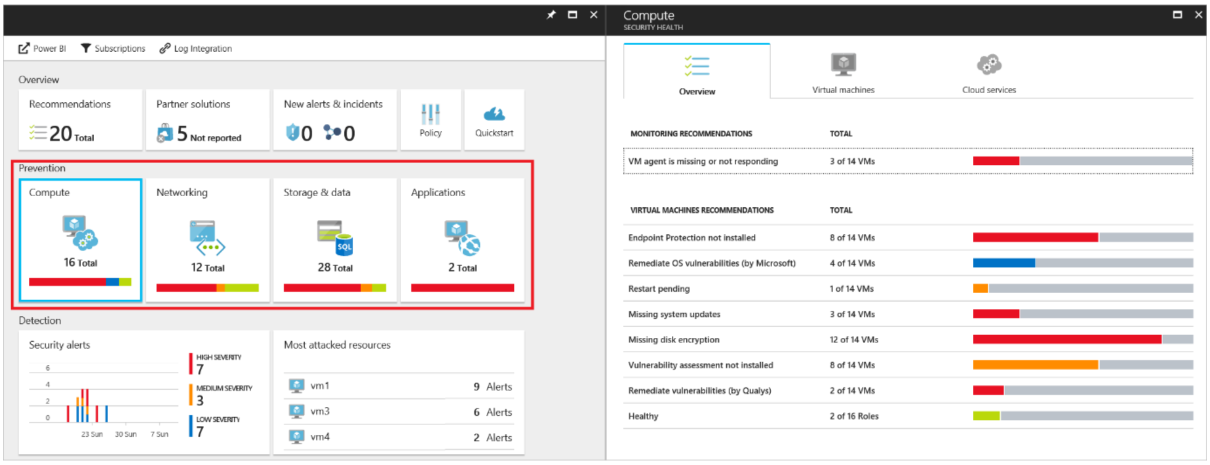
Recommendations

Filter

DESCRIPTION	RESOURCE	STATE	SEVERITY	
Enable VM Agent	3 virtual mac...	Open	❗ High	...
Install Endpoint Protection	8 virtual mac...	Open	❗ High	...
Add a web application firewall	2 web applic...	Open	❗ High	...
Add a Next Generation Firewall	6 endpoints	Open	❗ High	...
Finalize Internet facing endpoint protec...	VM3-RDP-M...	Open	❗ High	...
Enable Network Security Groups on sub...	3 subnets	Open	❗ High	...
Enable Network Security Groups on virt...	vm1classic	Open	❗ High	...
Route traffic through NGFW only	vm3	Open	❗ High	...
Enable Auditing & Threat detection on...	sqlserver1as...	Open	❗ High	...
Remediate vulnerabilities (by Qualys)	2 virtual mac...	Open	❗ High	...
Enable Auditing & Threat detection on...	2 SQL datab...	Open	❗ High	...
Apply a Just-In-Time network access co...	7 virtual mac...	Open	❗ High	...
Apply system updates	3 virtual mac...	Open	❗ High	...
Apply disk encryption	12 virtual ma...	Open	❗ High	...
Enable encryption for Azure Storage Ac...	19 storage a...	Open	❗ High	...
Restrict access through Internet facing...	6 virtual mac...	Open	⚠ Medium	...
Add a vulnerability assessment solution	8 virtual mac...	Open	⚠ Medium	...

MONITOR

Instantly on the Security Centre home page, the largest tiles in the centre of the screen are the ‘Security State’ icons - these give a brief summary of your entire cloud network, and the level of protection you have on each computing, virtual networks, storage, and your hosted applications. If you click on any one of these, you can get a more detailed breakdown for each section.



MONITORING RECOMMENDATIONS	TOTAL
VM agent is missing or not responding	3 of 14 VMs

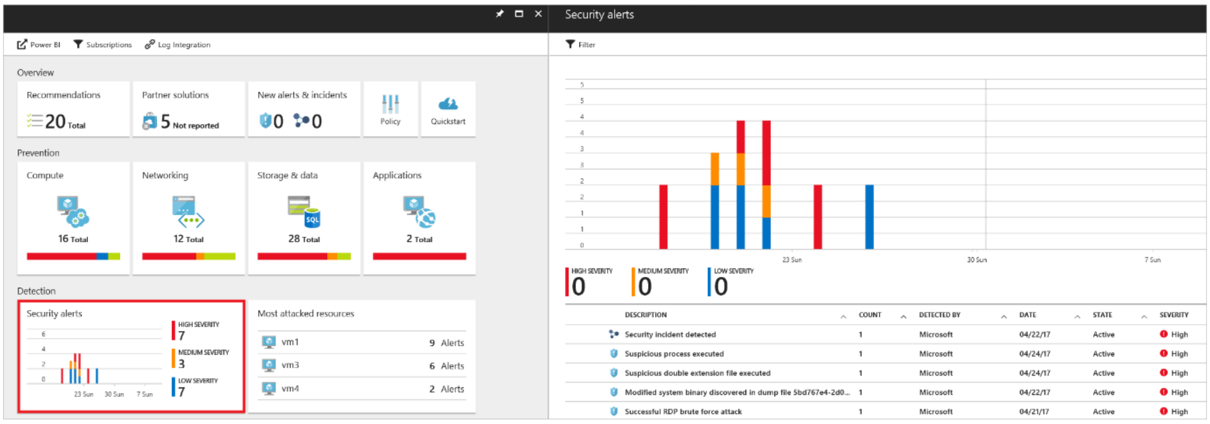
VIRTUAL MACHINES RECOMMENDATIONS	TOTAL
Endpoint Protection not installed	8 of 14 VMs
Remediate OS vulnerabilities (by Microsoft)	4 of 14 VMs
Restart pending	1 of 14 VMs
Missing system updates	3 of 14 VMs
Missing disk encryption	12 of 14 VMs
Vulnerability assessment not installed	8 of 14 VMs
Remediate vulnerabilities (by Qualys)	2 of 14 VMs
Healthy	2 of 16 Roles

REACT

The security alerts tile will create alerts when threats are detected by software such as anti-malware programs and firewalls. Security alerts could be triggered for varying reasons, such as:

- Compromised VM’s communicating with known malicious IP addresses.
- Advanced malware detected by using Windows error reporting.
- Brute force attacks against VM’s.
- Security alerts from integrated anti-malware programs and firewalls.

The Security Centre will prioritise security alerts, and give suggestions on how to react to them when you click on them.



DESCRIPTION	COUNT	DETECTED BY	DATE	STATE	SEVERITY
Security incident detected	1	Microsoft	04/22/17	Active	High
Suspicious process executed	1	Microsoft	04/24/17	Active	High
Suspicious double extension file executed	1	Microsoft	04/24/17	Active	High
Modified system binary discovered in dump file 5bd767e4-2d0...	1	Microsoft	04/22/17	Active	High
Successful RDP brute force attack	1	Microsoft	04/21/17	Active	High

STATISTICS

Data collected by the security centre will allow you to identify the weaker, or more frequently targeted points within your system - and allow you to take further preventative steps to safeguard your network.

The statistics collected can provide an overview of any potential flaws in your cloud network, and allow you to prioritise based on what is important to you.

Cybersecurity in AWS

Data protection

AWS provides services that help you protect your data, accounts, and workloads from unauthorized access. AWS data protection services provide encryption and key management and threat detection that continuously monitors and protects your accounts and workloads.

Identity & access management

AWS Identity Services enable you to securely manage identities, resources, and permissions at scale. With AWS, you have identity services for your workforce and customer-facing applications to get started quickly and manage access to your workloads and applications.

Network & application protection

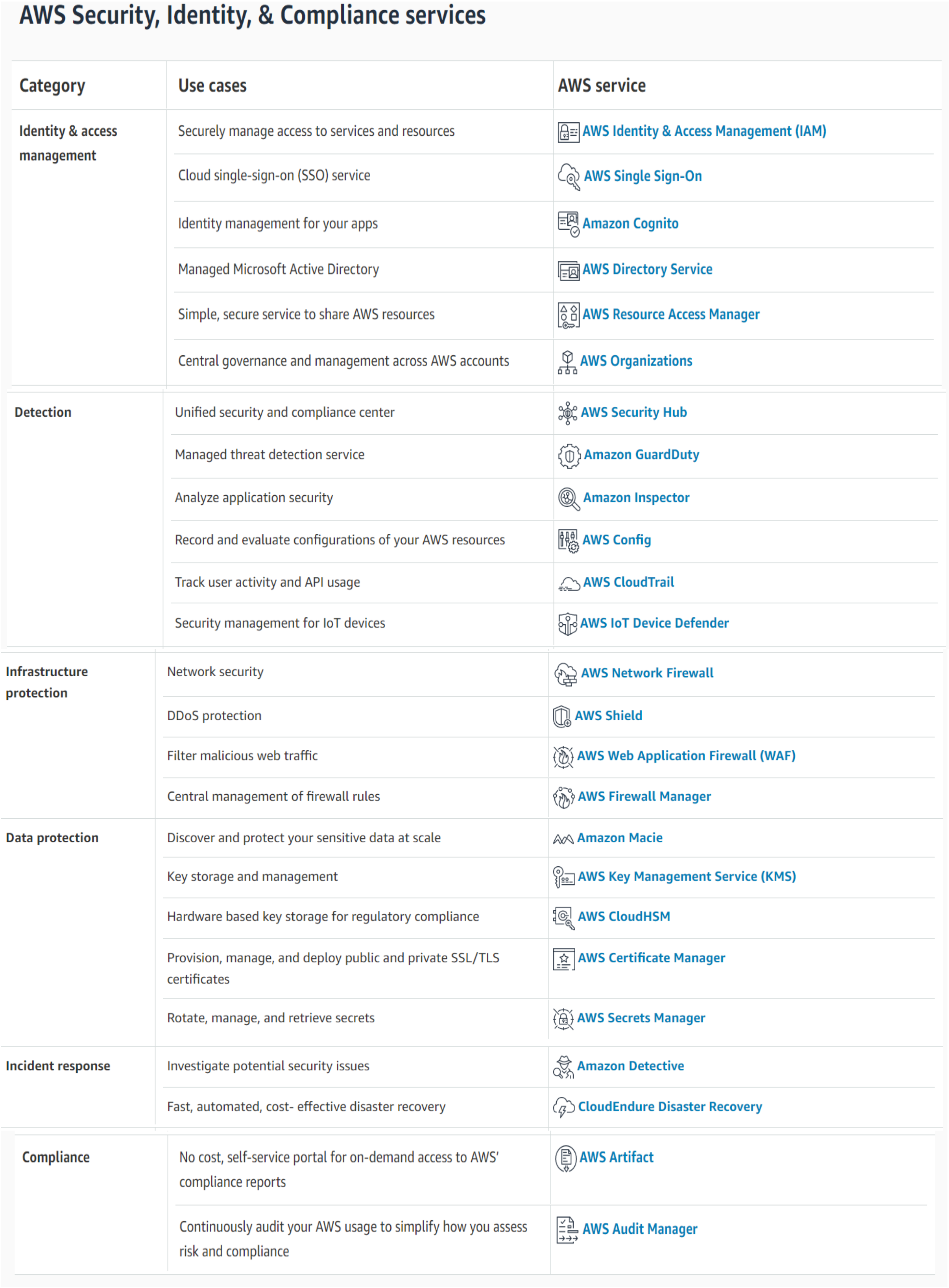
Network and application protection services enable you to enforce fine-grained security policy at network control points across your organization. AWS services help you inspect and filter traffic to prevent unauthorized resource access at the host-, network-, and application-level boundaries.

Threat detection & continuous monitoring

AWS identifies threats by continuously monitoring the network activity and account behaviour within your cloud environment.

Compliance & data privacy

AWS gives you a comprehensive view of your compliance status and continuously monitors your environment using automated compliance checks based on the AWS best practices and industry standards your organization follows.



AWS Security, Identity, & Compliance services

Category	Use cases	AWS service
Identity & access management	Securely manage access to services and resources	AWS Identity & Access Management (IAM)
	Cloud single-sign-on (SSO) service	AWS Single Sign-On
	Identity management for your apps	Amazon Cognito
	Managed Microsoft Active Directory	AWS Directory Service
	Simple, secure service to share AWS resources	AWS Resource Access Manager
	Central governance and management across AWS accounts	AWS Organizations
Detection	Unified security and compliance center	AWS Security Hub
	Managed threat detection service	Amazon GuardDuty
	Analyze application security	Amazon Inspector
	Record and evaluate configurations of your AWS resources	AWS Config
	Track user activity and API usage	AWS CloudTrail
	Security management for IoT devices	AWS IoT Device Defender
Infrastructure protection	Network security	AWS Network Firewall
	DDoS protection	AWS Shield
	Filter malicious web traffic	AWS Web Application Firewall (WAF)
	Central management of firewall rules	AWS Firewall Manager
Data protection	Discover and protect your sensitive data at scale	Amazon Macie
	Key storage and management	AWS Key Management Service (KMS)
	Hardware based key storage for regulatory compliance	AWS CloudHSM
	Provision, manage, and deploy public and private SSL/TLS certificates	AWS Certificate Manager
	Rotate, manage, and retrieve secrets	AWS Secrets Manager
Incident response	Investigate potential security issues	Amazon Detective
	Fast, automated, cost- effective disaster recovery	CloudEndure Disaster Recovery
Compliance	No cost, self-service portal for on-demand access to AWS' compliance reports	AWS Artifact
	Continuously audit your AWS usage to simplify how you assess risk and compliance	AWS Audit Manager

Cybersecurity in GCP

Google Data Center security on the physical note- When it comes to the protection of its data center assets, the Alphabet Inc's subsidiary seems to be very serious. The company is seen protecting its infrastructure with the help of biometric detectors, alarms, cameras, security lasers with minimalistic human indulgence. So, as everything is automated at this segment, errors are almost negligible or mere zero.

Highly customized Hardware and Software- Google has announced to the world in the year 2015 that it builds its hardware like server boards, networking devices, and customized server machines- all as per its needs and security requirements. And when it comes to software's like firmware stack, curated OS images, and hardened hypervisors are all tuned as per its requirements.

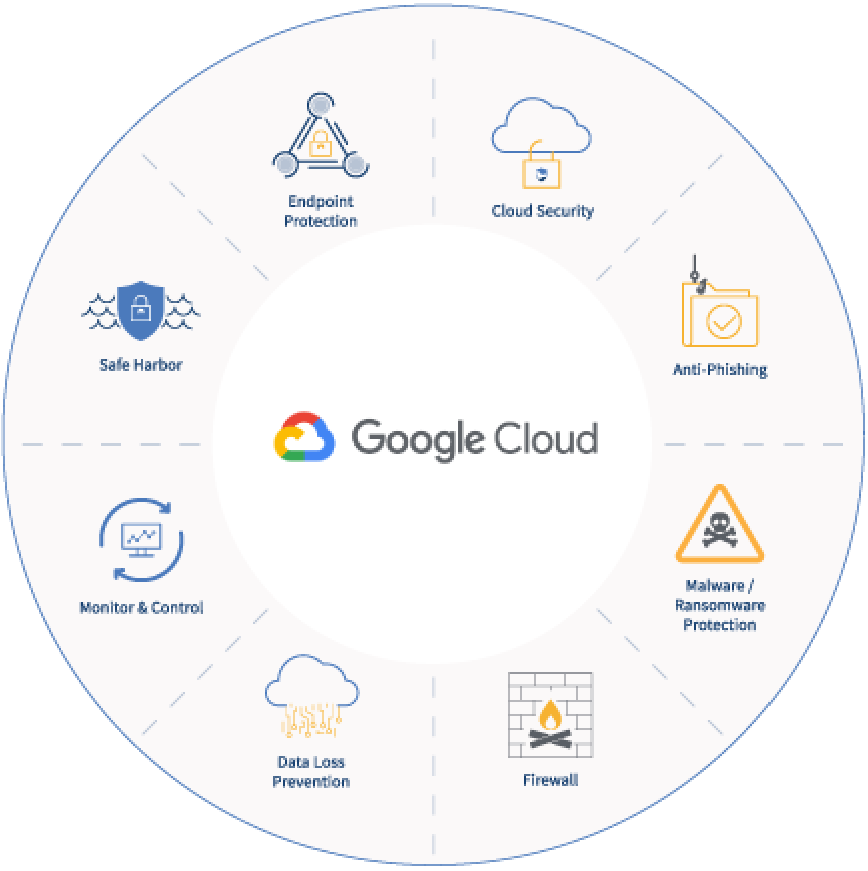
Data storage and destruction- As the Sundar Pichai firm happens to have tons of Petabytes of data moving to and fro, at the end of the data it also has to do persistent disk cleanups to make way for the new lot. Google says that data destruction at its premises is done scientifically by using a logical disk cleaning technique for cleanups and the results of erasure are securely stored and logged in the disks in a perfect way for future weekly audits. Then the erased disk is released into the inventory for reuse.

Data encryption- is also done at two points on GCP. As the encryption is automatic it requires no action from the user's side. An AES- 256 algorithm is applied with master keys which are again termed by the Google servers.

Network monitoring, data access monitoring, intrusion detention are all kept operational at the server farms of Google. DDoS protection, login abuse protection, and authentication are being given a priority by the tech giant these days.

GOOGLE CLOUD PLATFORM INFRASTRUCTURE SECURITY FEATURES INCLUDE:

- 24/7/365 operations, device security detection and response from both internal and external threats
- Data in-transit encrypted communication to and from Google's public cloud, including layered defense redundancies to protect customers from denial-of-service (DoS) attacks
- Identity protection and management through multiple authentication factors
- Data at-rest storage security using encryption against unauthorized access and distribution for reliability
- An entire hardware infrastructure created, built, controlled, and secured by Google including servers, networking equipment, and security chips



References:

1. https://www.reply.com/solidsoft-reply/en/content/protection-in-the-cloud-cybersecurity-in-azure
2. https://aws.amazon.com/products/security/
3. https://www.cybersecurity-insiders.com/security-features-on-google-cloud-platform-gcp/
4. https://managedmethods.com/blog/google-cloud-platform-security-features/