ClearVision

SECURITY PROTOCOLS FOR ClearHost

CONTENTS

USER NOTICE

Customers are responsible for making their own assessment of the information outlined in this document.

This document:

(a) is for informational purposes only, (b) represents the current ClearHost offering which is subject to change without notice, and (c) does not create any commitments or assurances from Clearvision and/or its affiliates, suppliers or licensors. The responsibilities and liabilities of Clearvision to its customers are controlled by Clearvision agreements, which this document is not part of, nor does it modify any agreement between Clearvision and its customers.

This document is intended to answer questions, such as how Clearvision keeps customer data secure in its hosted environment ClearHost, and more specifically, describes the physical and operational security processes for its server infrastructure under the management of Clearvision on Amazon Web Services (AWS).

INTRODUCTION

The more humanity depends on technology, the more important security becomes. Businesses originally opted for cloud to save money, but with the evolution of the digital age, security has become the motivator.

As a cloud-first pioneer, Clearvision is well-equipped in understanding the security implications of the cloud model, with hosted services designed to deliver better security than most traditional on-prem solutions.

At Clearvision, security is a top priority. They run their servers on the same infrastructure as their customers as it's vital to their everyday operations where threats are concerned. It's the cornerstone of their account controls, and compliance audits as part of the ISO 27001 certification they achieved in 2019.

This white paper outlines their approach to security and compliance for their hosted cloud solution, ClearHost, and the software apps involved. Readers of this paper will get a transparent overview of how Clearvision handles and protects customer data.

SHARED RESPONSIBILITY MODEL

Security in the cloud differs from security in on-premise data centers, as when computer systems and data are migrated to the cloud, security becomes a shared obligation. For example, where ClearHost is concerned, Clearvision, the customer, and the cloud service provider (AWS), all share the responsibility of data. AWS and Clearvision handle the underlying infrastructure that supports cloud, while the customer in question takes care of anything that's added or connected. This shared responsibility model reduces the customer's operational burden in a number of ways, and in some cases even improves default security posture without the need for additional action.

AWS	HARDWARE/AWS GLOBAL INFRASTRUCTURE			
	Regions	Availability Zones	Edge Locations	
	SOFTWARE AND SERVICES			
	Compute	Storage	Database	Networking

Clearvision	PLATFORM AND APPLICATIONS			
	Operating System	Security Patching	Vulnerability Management	Application Installation Database Administration
	NETWORK			
	Security Groups/ Firewall	Subnets	VPC	Network ACL Intrusion Detection And Pre-vention
	DATA AND BACKUP			
	Snapshot Backups	Data Volumes	Encryption At Rest	Data Transfer

Customer	POLICY AND COMPLIANCE
	Ensuring that the system meets your business needs and is operated in accordance with industry, regulatory and legislative compliance obligations.
	USERS
	The creation and management of user accounts.
	INFORMATION
	The content stored within ClearHost applications.
	MARKETPLACE APPS/PLUGINS
	Third-party services that require access to your information including how they integrate with ClearHost products.

AWS SECURITY RESPONSIBILITIES

Amazon Web Services is responsible for protecting the global infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure comprises the hardware, software, networking, and facilities that run AWS services. Protecting this infrastructure is the number one priority of AWS.

Although you cannot visit their data centers or offices, several reports from third-party auditors are available to verify their compliance with a variety of computer security standards and regulations.

CLEARHOST SECURITY RESPONSIBILITIES

With the AWS Cloud, ClearHost provisions virtual servers, storage, databases, and networks. AWS products that fall into the well-understood category of Infrastructure-as-a-Service (IaaS), such as Amazon EC2, and Amazon VPC, are under Clearvision's control, for which all of the necessary security configuration and management tasks are performed. As an example, for EC2 instances, Clearvision is responsible for managing the guest OS (including updates and security patches), any application software or utilities installed on the instances, and the configuration of the AWS provided firewall (called a security group) on each instance. AWS managed services such as Amazon RDS, provides all of the resources ClearHost needs to perform a specific task — but without the configuration work that comes with it. With managed services, launching and maintaining instances isn't necessary, nor is patching the guest OS or database, or replicating databases, as AWS handles it all.

CUSTOMER SECURITY RESPONSIBILITIES

Customers are responsible for managing the information and data within their accounts, the users and user accounts accessing data. Marketplace apps (formerly add-ons) also come under this responsibility. When using Atlassian applications provided for by Clearvision, customers are responsible for ensuring that their business meets compliance obligations.

RESPONSIBILITIES INCLUDE:

- **Policy and compliance:** Ensuring that the system meets business needs and is operated in accordance with industry, regulatory and legislative compliance obligations.
- **Users:** The creation and management of user accounts.
- **Information:** The content stored within applications.
- **Marketplace apps:** Third-party services that have access to information, and their ability to integrate with other products.

SECURITY AS A CULTURE

Clearvision has an active and comprehensive security culture that is introduced to employees at the onboarding stage.

Their Information Security Management System (ISMS) is ISO 27001 certified, which is the leading international standard to have in the world for Information Security Management Systems. This accreditation provides a holistic approach to information security by assessing the risk of people, processes and IT systems.

The standard allows them to protect the confidentiality of assets, and maintain the integrity of data and the availability of IT systems whilst reducing disruption risks.

They are also Cyber Essentials certified which is a government-backed scheme built to protect organisations against the threat of cyber attacks.

Their efforts to obtain high-level security standards has instilled confidence in their customer base, as vital knowledge is not limited to key stakeholders, with employees undergoing training to ensure they adhere to the requirements of security best practices. Refresher training is compulsory for staff and must be completed on an annual basis. Clearvision employees are also encouraged to refer to the documentation policies and procedures that outline business continuity plans, risk management, etc. which are available on Confluence — their collaboration wiki tool.

EMPLOYEE BACKGROUND CHECKS

HR ensures that all candidates, regardless of whether they are permanent or temporary are screened appropriately. Before employees are onboarded, checks are performed based on their education and employment history. Any internal or external references provided by the candidate are also contacted. The extent of such background checks varies according to the position in question.

SECURITY TRAINING

Employees at Clearvision must participate in security training as part of the onboarding process which is refreshed annually. Depending on their responsibilities, additional training on specific aspects of security may be required. An example of this would be members of the IT team who instruct new engineers on topics such as the management of technical vulnerabilities.

INTERNAL AUDIT AND COMPLIANCE ROLES

ClearHost uses a dedicated third party to review compliance with security laws and regulations around the world. As new auditing standards are created, controls, processes, and systems are determined. Clearvision facilitates and supports independent audits and assessments from third parties where required.

OPERATIONAL SECURITY

VULNERABILITY MANAGEMENT

Clearvision has vulnerability management practices in place to proactively prevent exploitation and the loss of sensitive data. Clearvision may create and document systematic and accountable practices to maintain control programs and applications, for the purposes of evaluating installed and new devices and systems for vulnerabilities. This is also to mitigate other technical and non-technical threats. The goal of this is to provide an added layer of protection for Clearvision's IT resources and to ensure the compliance of best practices to reduce the impact of threats to Clearvision and its customers.

INTRUSION DETECTION AND PREVENTION

Clearvision utilises GuardDuty across its AWS estate. Amazon GuardDuty is a threat detection service that continuously monitors malicious activity and unauthorised behaviour to protect AWS accounts and their workloads, including servers. With GuardDuty, Clearvision has an intelligent option for continuous threat detection in the AWS Cloud. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritise potential threats. GuardDuty analyses tens of billions of events across multiple AWS data sources, including AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs.

The IT Operations team receives automated tickets logged for alerts from GuardDuty for medium/high risks.

ATLASSIAN APPLICATION VULNERABILITIES AND SECURITY ADVISORIES:

LOGGING AND TRACKING SECURITY ADVISORIES

Clearvision tracks all critical-severity security vulnerabilities, by monitoring the issue trackers for the relevant products on https://jira.atlassian.com. For example, https://jira.atlassian.com/browse/JRA for Jira and https://jira.atlassian.com/browse/CONF for Confluence. Security issues in trackers are marked with a security label. All security issues are listed in the release notes to state where they have been fixed.

As an Atlassian Platinum Solution Partner, Clearvision receives security alerts which are tracked via the Partner Portal before public release. This ensures that the correct mitigation and patching methods are in place before public distribution. Clearvision internally tracks, communicates, patches, and mitigates critical security vulnerabilities via Jira Service Management.

MONITORING AND CAPACITY MANAGEMENT

Clearvision hosted systems have a tool to proactively monitor all hosted systems including network bandwidth, server memory, CPU and disk space utilisation.

Actions for each type of alert are defined in an internal alert management process. For high alerts, tickets are logged via the internal Service Desk where they are actioned. Any concerns are discussed in weekly meetings.

Changes to the ClearHost network or servers follow the IT Change Management Process.

Any instances where capacity has breached the pre-defined limitations are highlighted and documented in the meeting minutes.

INCIDENT MANAGEMENT

Clearvision operates a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems and data. If an incident occurs, the security team logs and prioritises it according to severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation.Clearvision's security incident management policy is aligned with ISO 27001 best practices.

CONCLUSION

Data protection is a primary design consideration for the infrastructure, products and personal operations of Clearvision.

Clearvision's hosted cloud solution ClearHost, along with AWS, offers a level of protection that very few public cloud providers or IT teams are able to match.

Amazon Web Services — the world's most trusted provider powers ClearHost, which gives our customers peace of mind. Listen to our podcast episode on the story of our partnership for more information.