

CyberHive Trusted Cloud

Secure hosting for sensitive workloads in the cloud or on premises

Easily deploy sensitive workloads in the cloud or on premises while saving an average of two-person months per project



Time and cost savings

Automate repeatable configuration-as-code solutions



Ultimate assurance

Instant detection of intrusion or malicious changes



Enhance security

Government approved to handle sensitive workloads up to 'Official-Sensitive'

Why CyberHive Trusted Cloud?

Businesses worldwide have an aspiration to move towards cloud-hosted infrastructure to gain the benefits of reduced cost and increased flexibility. This is slowed by the need to ensure that all new services are adequately protected from attack by cyber criminals, hackers or other digital adversaries.

Furthermore, for critical or confidential information where an elevated level of security is required, the necessary governance to ensure that security measures are well defined and properly implemented can dramatically increase costs and bring new in-house projects to a standstill.

Rapid deployment with CyberHive Trusted Cloud

Trusted Cloud gives organisations the ability to host their sensitive applications in protected public cloud instances and cut development and deployment costs by up to 70%.

Built using a tried and tested architecture and incorporating novel techniques and technologies, CyberHive's Trusted Cloud provides a turn-key solution for hosting any workload. It has been validated by a government-appointed third party to handle information up to "Official-Sensitive" classification and higher sensitivity workloads can be easily accommodated.

Our standardised approach to security, massively cuts the cost of developing new services and reduces the time needed to implement new deployments. This approach provides instant and enhanced security together with audit trail capabilities, for any workload that can be run in the cloud to protect applications, users and data.

By providing a pre-approved framework into which new business applications can be easily spun up, standing up a new workload is a rapid process. The framework uses templates (utilising industry-leading tools such as Terraform) freeing up your business to move forward quickly, safe in the knowledge that the secure infrastructure will protect deployed applications now and into the future.

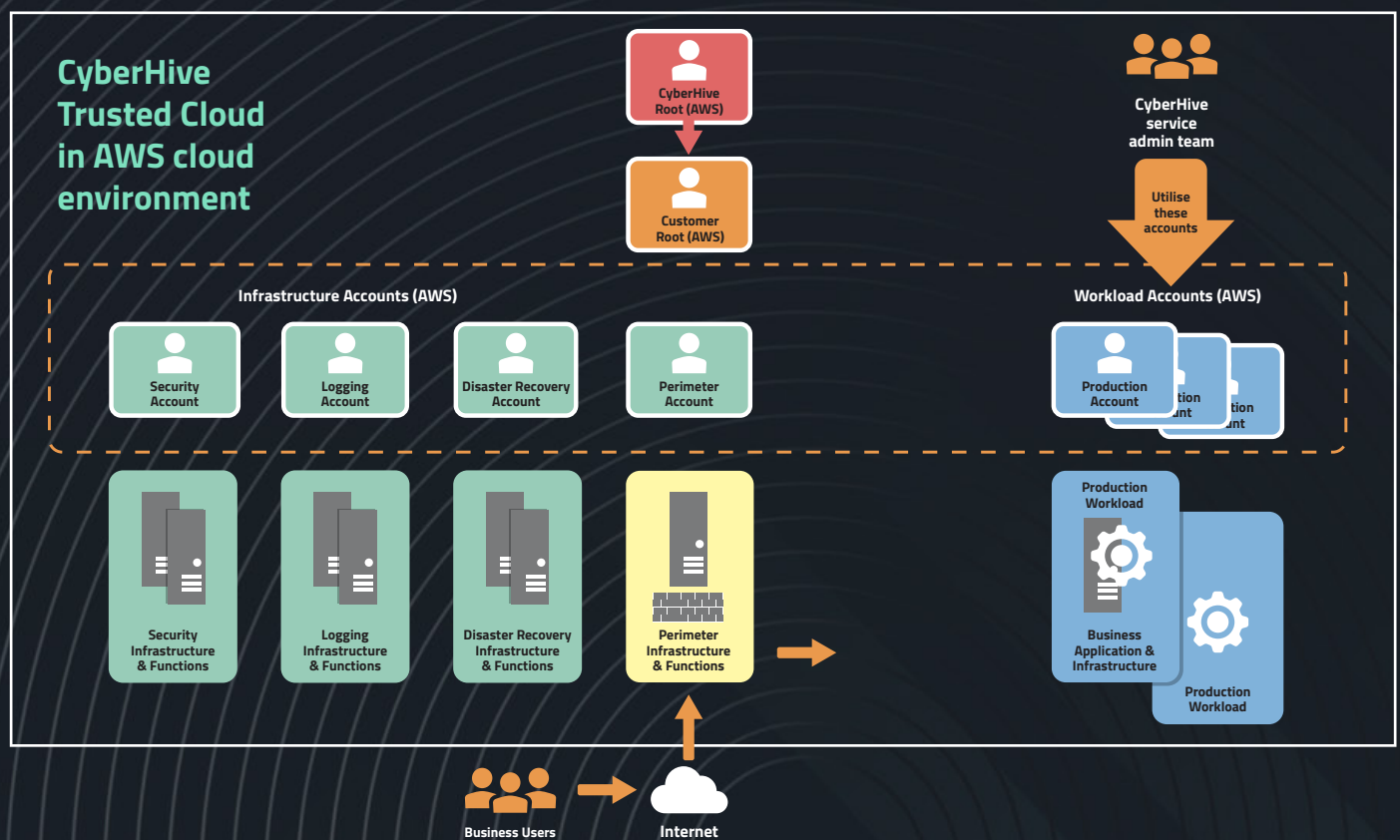


Segregated by design - system architecture

Trusted Cloud is implemented as a virtual private cloud on Amazon Web Services (AWS) for your business. The pre-defined and approved architectural framework consists of all the functionality required to wrap enhanced security around your business applications that run as workloads. CyberHive will deploy these in accordance with the requirements of your chosen applications and users. CyberHive will then provide everything as a service backed by a skilled administrative team, taking care of patching, updates and monitoring cloud resources and status.

Trusted Cloud meets all 14 of the National Cyber Security Centre (NCSC) Cloud Security Principles aligned to ISO27017 and is independently reviewed for 'Official-Sensitive' data. **Trusted Cloud** Infrastructure maybe further secured by our patented Trusted Compute technology which we developed in collaboration with the University of Oxford to attest the cloud instances. It significantly reduces the time it takes to detect and locate data breaches down to seconds. Rapid detection has a very strong case when considering where to prioritise efforts to increase cyber resilience. The less time hackers and malicious insiders are left to probe around your network unchallenged the better.

The following figure summarises the overall architecture, with the supporting functions shown in green and the multiple application workloads in blue, with the access point in yellow. All infrastructure accounts are derived from a customer specific root account.



The core tenet of the architecture is the segregation of functions, by design these are separated into specific AWS infrastructure accounts. This provides a logical separation between different aspects of infrastructure which limits an internal threat actor from affecting resources outside the scope of their access.

The infrastructure accounts are:

Security account

Provides administrator access to the security tools and supports monitoring of the AWS infrastructure activity.

Logging account

Places log files into immutable storage from the AWS infrastructure to support a forensic capability.

Disaster recovery account

Stores backups of AWS infrastructure and configurable workload content to ensure these cannot be corrupted by malicious activity.

Perimeter account

Manages key infrastructure for mediating system access between business users, applications and data.

Workload accounts

Hosts any number of separately managed and securely isolated business user applications.

These key infrastructure accounts, with their functions and equipment are therefore only accessible to the CyberHive administrative team with corresponding roles and privileges, thus enforcing separation of duty.

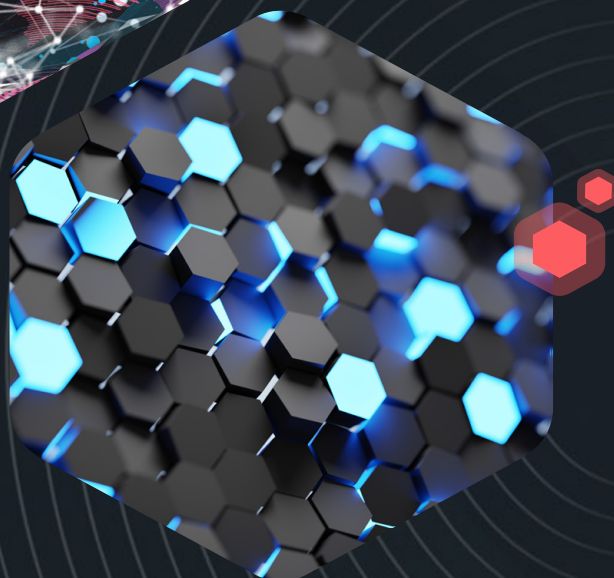
Controlled access

Business user access to and from **Trusted Cloud** is controlled at a single point – the perimeter account. This gateway delivers:

- control of external and internal traffic via a pair of highly available EC2 firewall nodes sitting across the internal infrastructure subnets;
- traffic routing to the appropriate workload account to allow the user to access the business application;
- load balancing to ensure efficient traffic flow at the network and application layers;
- outbound connectivity with backend applications.

The user's experience of accessing the business applications is transparent, and they continue to use the account credentials as normal.

Administration by the CyberHive team is carried out using the dedicated AWS administration accounts.



Delivered with key protective components

The **Trusted Cloud** architecture has been purposely designed to deliver security for business data, simplicity for business operations and ultimately, greater business agility. As such it features many industry-leading and trusted components to simplify management, operation and monitoring. These trusted architectural components include:

- **Amazon GuardDuty** – this threat detection service constantly monitors the activity in AWS for anomalous behaviour that could indicate a cyber attack or other unauthorised use;
- **AWS Security Hub** – collects data across all Trusted Cloud AWS accounts and provides a comprehensive view of the security state of the AWS environment;
- **AWS CloudTrail** – supports compliance, operational and risk auditing of AWS accounts. Actions taken by a user, role or AWS service across all the Trusted Cloud accounts are recorded under the logging account;
- **Amazon CloudWatch** – monitors resources deployed across all the Trusted Cloud AWS accounts by collecting logs and tracking metrics. Trusted Cloud includes custom dashboards to display metrics and alarms to notify administrative users of specified changes or events;
- **Immutable storage** – used for security logs;
- **Veeam Backup for AWS** – delivers fully automated backup and disaster recovery;
- **Secure perimeter** - with resilient AWS EC2 firewall nodes;
- **AWS Shield** - provides protection against a wide range of known distributed denial-of-service (DDoS) attack vectors and zero-day attack vectors.

CyberHive

With over 20 years' experience, CyberHive brings you a new standard in cyber security.

Helping to protect your data not only from external threats, but also from any security lapses by employees, which could damage your business reputation and even result in a loss in revenue.

CyberHive offer innovative, scalable and secure solutions including the award winning CyberHive Trusted Cloud, CyberHive Gatekeeper for Microsoft 365 and CyberHive Connect.


Cyber security is not just a technology decision, it's a business decision.



Act now and get in touch

Don't leave your organisation open to attack, safeguard your cloud workloads, critical connections, and sensitive data today.

Contact info@cyberhive.com or visit www.cyberhive.com to find out how CyberHive can protect your business.

 01635 881880

 info@cyberhive.com

 www.cyberhive.com



CyberHive
2nd Floor, Newmarket House
Market Street,
Newbury,
Berkshire RG14 5DP