cyberhive

The perfect new key to total cloud security –

Trusted Cloud by CyberHive

CyberHive's unique new combination of hardware-based cryptography and whitelisting technology protects servers from all unauthorised activity and malware in a way that conventional solutions can never match

Trusted Cloud in a nutshell What do you get?

Firstly all the benefits of our world-class cloud platform that include:

- Self-service cloud platform
- Flexible hourly charging for servers and storage – only pay for what you use
- Advanced software-defined networking
- Reduced capex for IT equipment
- Improved reliability and resilience
- Ability to connect from anywhere
- Data only held in UK datacentres
- MPLS networking options
- High speed redundant internet connections
- One complimentary IPv4 address included with each account
- Additional service options that includes load balancers; virtual routing; firewalls; VPNs and auto-scaling

On top of these benefits, Trusted Cloud gives you the best server protection available.

It offers:

- Heightened security through advanced use of distributed whitelisting that defeats hackers, malicious admins and eliminates devastating effects of security lapses
- No single person or organisation can rig the system, tamper with servers or bypass security
- Automatic verification of server integrity every five seconds by multiple servers rapidly identifies unauthorised software or hardware
- Unhackable transmission using the cryptographic power of Intel's TPM chip to prevent falsification of verification data
- Flexible and scalable – verification can be conducted anywhere in the world in total independence from your cloud service provider
- Trusted Cloud is based on 100 IT's self-service cloud platform, managed through easy-to-use, comprehensive dashboards
- Trusted Cloud is also available for customers to deploy in their own on-premises datacentre

Why is cloud security such an important topic now?

Recent events show that a data hack is a nightmare for any organisation, whether the perpetrators are state-sponsored groups, malicious employees or corrupt staff at a cloud hosting provider.

Seemingly impeccable organisations such as Yahoo, TalkTalk, Sony PlayStation Network, the NHS and Equifax have all been hacked. Data relating to billions of individuals has been compromised, resulting in devastating reputational damage for the organisations and severe financial impact. According to new research published by Accenture and the Ponemon Institute, the average cost of cyber crime globally in 2017 climbed to $11.7 million per organisation.

The risks to any business are only going to increase with the advent of new regulatory regimes. The European Union's General Data Protection Regulation which came into force on 25th May this year (2018) imposes fines of up to four per cent of global turnover for organisations that have been breached or that fail to meet compliance requirements.

This ratcheting up of risks make cloud security an urgent necessity. But with conventional solutions all susceptible to hacking or falsification, Cyberhive has launched its new Trusted Cloud secure computing platform to set a new standard in security for data and applications held on servers, whether in the cloud or in an on-premises datacentre.

Co-developed with the University of Oxford, Trusted Cloud's patented technology employs the power of Intel's TPM chip, which is a dedicated micro-controller designed to secure hardware through integrated cryptographic keys. With its ability to detect unauthorised software or hardware in seconds, Trusted Cloud will immediately raise the alarm when servers or the underlying infrastructure have been compromised.

Why is Cyberhive's Trusted Cloud better than conventional solutions?

This new approach to cloud security is required because none of the conventional solutions is any longer capable of protecting an organisation's servers.

Let's consider the conventional options:

AV and firewalls are long-established but are effective against only the most basic of attacks. They cannot keep pace with hundreds of millions of new malware variants that hackers release every year. Criminals are finding it easier every day to deliver malware, especially through socially-engineered emails that tempt busy employees into clicking open links or macros that trigger zero-day attacks.

Disk encryption protects data at rest but necessitates the use of cryptographic keys when the data has to be used, opening up the possibility of unintentional security lapses by employees, or of malicious acts by server administrators. A server can still be compromised even if the disks are encrypted. Disk encryption alone is not the answer.

Network traffic analysis employs artificial intelligence (AI) to raise alerts about any rogue traffic on a server, reducing the chances of a successful brute force attack or substantial theft of data. The problem is that this technology relies on detecting major changes in use-patterns, which means a more precise attack can slip through, creating the ideal opportunity for a threat focused on a single weak-point to succeed.

Whitelisting ensures that only approved code is on a server. Its flaw however is the requirement for a list of what is running on a server to be transmitted (perhaps every minute) to a verification service. That information can be altered by hackers or malicious insiders in order to make it appear as if everything is in order, when in reality, client servers have been by-passed by targeted code or hit by a hypervisor attack.

The Cyberhive solution – **Trusted Cloud**

Resolving these challenges and providing a convincing solution in the face of the ever-growing range of threats can only be achieved through real innovation and insight.

That is why at Cyberhive we have designed Trusted Cloud – a next-generation platform that will work for any security-conscious organisation, from banks, financial institutions and governments to all companies concerned about data privacy legislation.

How is Trusted Cloud different?

Trusted Cloud is unique because it combines all the advantages of whitelisting with major advances in chip technology.

It works by employing the Intel Trusted Platform Module (TPM) chip which is already installed on server motherboards. The chip is a dedicated micro-controller, impervious to hacking and designed to secure hardware through integrated cryptographic keys. Trusted Cloud is the only solution that uses the immense cryptographic power of this chip.

This gives Trusted Cloud a crucial advantage over standard whitelisting solutions by using the chip's unique properties to digitally "sign" verification data. This is sent to multiple attestation servers every few seconds, confirming that nothing unauthorised is running on the client's server. As soon as anything untoward is revealed, remedial action can be taken immediately, killing off threats before any damage is done.

It offers a speed of reaction unmatched by other methodologies and runs outside the operating system, making it impossible to compromise either through the cloud server or by achieving physical access. This ensures the security of virtual servers and storage and provides a dramatically more secure system than any alternative technology, since the attestation servers can run checks on one another, eliminating the possibility of compromise from a single server affecting the entire platform.

The use of the TPM chip has another huge advantage – it allows data to be securely transmitted across the internet, since the digital signature makes it impossible to tamper with. In practical terms this means that verification can take place on multiple servers simultaneously anywhere in the world under the control of independent administrators. This eliminates any single point of attack and is a major gain in protection from external attack and security lapses.

If organisations wish to take security a step further, one or more attestation servers can be hosted in a third-party data centre, preventing tampering from the services-provider and even from in-house IT teams.

With servers that are backed up regularly across multiple UK-based datacentres, Trusted Cloud gives businesses complete peace of mind that their IT infrastructure is safe.

In fact protection from the intervention or negligence of human beings is one of the big advantages of Trusted Cloud.

Built-in resilience and total control

Built on Cyberhive's secure, resilient UK-based infrastructure, providing 100 per cent up-time SLAs, Trusted Cloud gives customers the power to verify and monitor their servers independently of their providers.

No longer do cloud users have to rely on assurances about the security of their data, they can check for themselves that their data is protected from all threats.

This is a new standard in cloud security

Cyberhive's Trusted Cloud is a major advance in security for all businesses working in the cloud.

It is a highly innovative, transformational level of security, producing a new standard for cloud security that is essential for any business fully committed to the protection of data and the maintenance of its own integrity, reputation and continued success.

For cloud service providers or institutions with their own private cloud this is the sole path to providing a service with rock-solid security that is resilient, scalable and dynamic.

CyberHive Ltd Wessex House ▪ Oxford Road ▪ Newbury ▪ Berkshire ▪ RG14 1PA
t 01635 881881 www.cyberhive.com