DATASHEET

Cloud Infrastructure Security Datasheet

At Touchstone Cloud, the data security of your business is our priority.

This document outlines the measures we take to ensure your business systems and business data are secure, available and invulnerable to attack. These measures are designed into the architecture of our hosting platform not just offered as an added extra, providing you with unrivalled service for your business.

touchstone CLOUD

TOUCHSTONE CLOUD

CLOUD SECURITY

Touchstone Cloud takes a multi-tiered approach to cloud security, combining proactive and reactive security services to safeguard our customers from cyber threats.

Touchstone Cloud utilises a complete distributed denial of service (DDoS) protection solution based on detection, diversion, verification and forwarding of malicious traffic to ensure total protection.

If a DDoS attack is launched against our service, business continuity is maintained by:

Detecting

...the DDoS attack and diverting the data traffic destined for the target device to a specific network appliance for treatment.

Analysing

...and filtering the bad data packets from the good data packets, preventing malicious traffic from impacting performance while allowing legitimate transactions to complete.

Forwarding

...the clean traffic to maintain business continuity and minimise impact on customer experience.

TOUCHSTONE CLOUD

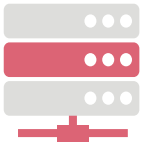
INTRUSION PREVENTION SYSTEM (IPS)

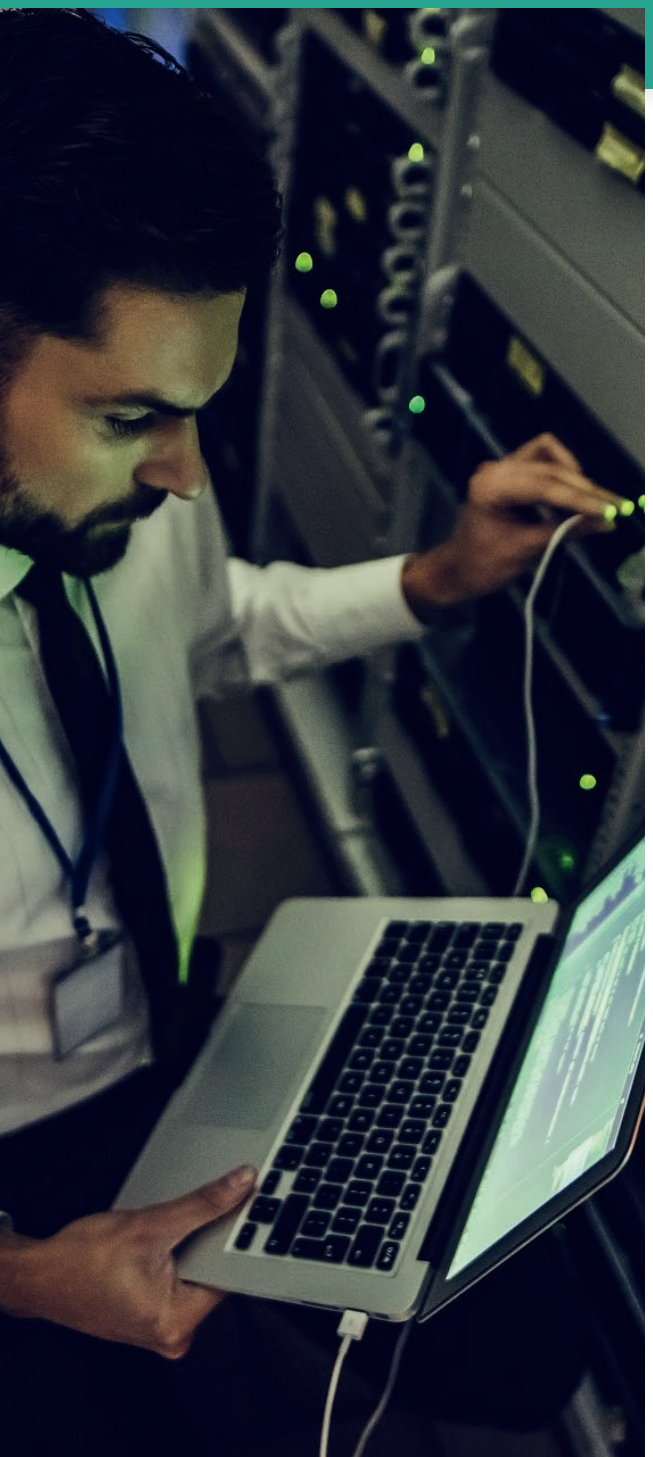
TouchstoneCloud utilises Fortinet technology via the industry validated and recognised FortiGate platform, providing the level of processing required to inspect all traffic with no impact on performance or network latency. It also includes industry leading threat intelligence from FortiGuard Labs, who have proven success in protecting from both known and zero-day threats.

If the IPS detects a suspicious data transfer, it will check the packets against a database of known viruses (Anti-Virus protection) to see if any malicious code is being transferred. Similarly, if an intrusion is detected, the IPS compares the activity to a set of rules designed to prevent malicious activities from taking place.

When an intrusion detection system (IDS) detects numerous failed logins, it may block the IP address from accessing any network devices. If it detects a virus, the data may be quarantined or deleted before it reaches its destination.

IPS is a key component of TouchstoneCloud's security fabric; It secures the entire end-to-end infrastructure without compromising performance or throughput.





TOUCHSTONE CLOUD

VIRTUAL ROUTING AND FIREWALLS (VRF)

Virtual servers are hosted on servers dedicated to Touchstone Cloud, with assured separation from other clients provided by the VRF solution. This ensures packets can only be routed between interfaces on the same VRF, improving security and network functionality within each local virtualised environment, as network paths can be segmented without requiring multiple routers.

This is backed up by a virtual firewall (VF) per customer instance, providing an additional layer of security, and additional packet filtering and monitoring within the Hypervisor itself.

Dependent on customer requirements, the VF can be installed as a traditional software firewall on a guest VM, or a purpose-built virtual security appliance designed with virtual network security in mind.

ADDITIONAL SECURITY MEASURES INCLUDE:

- Secure Antivirus web protection, protecting any web-based access from within the service
- ESET Server Antivirus software running automatically, in the background, on each server to prevent, scan and delete viruses, providing real time protection against a virus attack
- File server Crypto Locker protection is set up to lock users out before they can encrypt any files along with Shadow copy file recovery allowing users to easily recover files with previous versions
- Application control is used to ensure only approved applications can be installed or run
- Continuous patch management to minimise security
- Regular internal scans detect any vulnerabilities, flaws and bugs, preventing hackers exploiting out of date software to gain access to the system
- Encryption is used throughout the solution, maintaining data integrity in transit
- Full user account logging and auditing is available.

TOUCHSTONE CLOUD

BACKUP

File and SQL backups run nightly and are stored securely, following a 3-2-1 backup strategy.

This is made up of three rules:

3 copies of data

This includes the original data and at least two backups.

2 different storage types

Each copy of the backed-up data is kept on separate types of storage to minimize the chance of failure.

1 copy offsite

One data copy is stored in a secure or remote location to ensure that natural or geographical disasters cannot affect all data copies.

The **3-2-1 backup strategy** is recognised as a best practice for information security professionals and government authorities. While it does not guarantee all data will never be compromised, this strategy eliminates the most risk.

The **3-2-1 methodology** is important in ensuring that there is no single point of failure for data. Not only are our customers covered if one copy is corrupted or a technology fails, but also if a natural disaster or theft occurs that wipes out the physical storage types.

TOUCHSTONE CLOUD

DISASTER RECOVERY

Disaster Recovery (DR) involves a set of policies, tools, and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. Disaster Recovery assumes that the primary site is not recoverable (at least for some time) and represents a process of restoring data and services to a secondary, survived site enabling business continuity.

Touchstone Cloud services are deployed across 2 UK datacentres (also providing data sovereignty). Data is replicated every second between high performance Storage Arrays, across a dedicated datacentre to datacentre connection. DR invocation is tested monthly. In the event of a disaster in the primary location the customer server will only suffer a maximum of 1 second of data loss if our disaster recovery service is adopted.

PENETRATION TESTING

A penetration test is an authorised, simulated cyberattack on the TouchstoneCloud core system, performed specifically to evaluate the security of the system.

The test identifies weaknesses (also referred to as vulnerabilities), including the potential for unauthorised parties to gain access to the system's features and data.

This is run annually by an impartial third party and also identifies strengths within the service, enabling Touchstone Cloud Support to complete a full risk assessment on platform vulnerability.

TOUCHSTONE CLOUD

ACCREDITATIONS

The TouchstoneCloud platform is deployed within BlackBox Hosting's data centres. BlackBox Hosting is a key partner in maintaining TouchstoneCloud's security capabilities, providing the services described within this document.

They are committed to meeting and exceeding industry standards for IT business security, safety and continuity, as well as ensuring the environmental impact of those activities is accounted for and managed.

TO SHOWCASE THIS COMMITMENT, THEY HAVE INVESTED IN SIGNIFICANT WORLD - STANDARD ACCREDITATIONS INCLUDING:

CSA STAR LEVEL 2

The CSA STAR Certification is a third-party independent assessment of the security of a cloud service provider. The technology-neutral certification leverages the requirements of the ISO/IEC 27001:2013 management system standard together with the CSA Cloud Controls Matrix.

ISO 27001

BlackBox Hosting is fully ISO 27001 certified. The ISO 27001 standards help organisations to keep information assets such as financial information, intellectual property, employee details and third party information, secure. It guarantees that ample controls and other forms of risk treatment are in place to prevent and defend against potential vulnerabilities.

TOUCHSTONE CLOUD

ACCREDITATIONS cont...

CYBER ESSENTIALS +

This is a Government-backed scheme that helps to protect organisations and their customers, against a whole range of the most common cyber-attacks. BlackBox Hosting is Cyber Essentials Plus certified. The 'Plus' scheme requires companies to pass a more hands-on technical verification process to be awarded the certification.

ISO 20000-1

BlackBox Hosting maintains a Service Management Service (SMS) that is certified to ISO 20000-1 standards.

ISO 22301

This allows BlackBox Hosting to demonstrate commitment to achieving the highest available international standard for business continuity management. This demonstrates they have the required systems in place to support both Touchstone Software and our customers, and for the provision of SaaS (Software as a service).

ISO 9001

BlackBox Hosting has a Quality Management System (QMS) in place to ensure that they supply products and services that meet both regulatory requirements and the expectations of our clients. The QMS is certified to the ISO 9001 standard and is reviewed and updated on a regular basis to help ensure that they continue to meet and exceed expectations.

G-Cloud 12

BlackBox Hosting is a government approved cloud service supplier through the G-Cloud 12 framework. For public sector departments, procuring services through the G-Cloud framework is more efficient.

ISO14001

Blackbox Hosting and TouchstoneCloud are committed to reducing their impact on the environment. Blackbox Hosting holds the ISO14001 certification and is utilising this framework to achieve the goal of becoming carbon neutral as a business by the end of 2022.

touchstone
CLOUD

www.touchstonecloud.co.uk

+44 (0)20 7121 4702

46 Worship Street, London, EC2A 2EA