Infrascale™

THE SURVEILLANCE-PROOF CLOUD

TRUE SECURITY WITH ULTRASAFE

Technology Brief

UltraSafe Technology Delivers Triple-Stage Encryption for True Cloud Security

Protecting your data from the preying eyes of hackers and unwanted surveillance is now a fundamental requirement in today's cloud solutions. Infrascale's platform is uniquely built to deliver a truly surveillance-proof cloud.

Infrascale™

How It Works

STAGE 01

Infrascale encrypts your files using UltraSafe 256-bit AES, before transferring them to the cloud.

- Each user's files are secured with a unique UltraSafe encryption key.

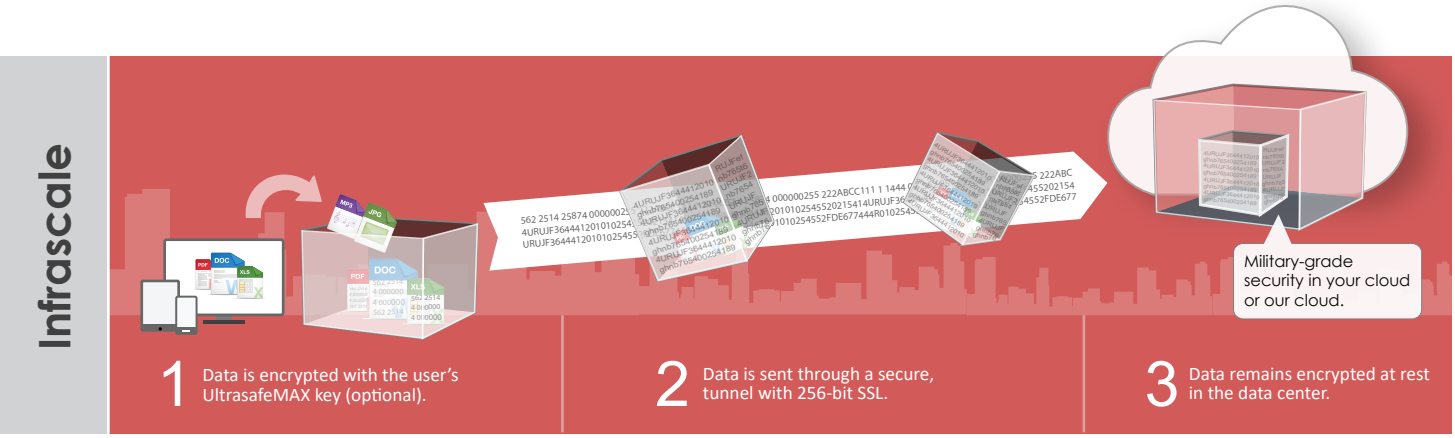
STAGE 02

Files are transferred to/from the cloud via a Secure Sockets Layer (SSL) connection. (This encryption key is stored on the local machine only, NOT in the cloud.)

STAGE 03

Data files stored in the Infrascale cloud are encrypted again with 256-bit AES encryption.

Your data files can only be decrypted by using the user-specific key stored on your local PC.



Triple-Stage Encryption means:

- With UltraSafe, encryption keys are NEVER stored or saved in the cloud. Absolutely no one is able to access data files, except for the account holder.
- Infrascale cannot access your data in any readable format. Even under court order.
- Data stored via UltraSafe in the Infrascale cloud cannot be read without your unique, private key. Which is kept only on your local machine.

Infrascale™

The Infrascale Cloud Security Strategy

Our cloud security approach covers the five essential stages of security – PLUS two additional fields.

- For Data Security and Transmission Security, see *Encryption & Key Management.*
- For Access Security, see *Access Controls, Monitoring and Audit Trails.*
- For Network Security, see *Deployment Flexibility and Secured Infrastructure.*
- For Physical Security, see *Secured Infrastructure.*

PLUS

- For Data Leak Prevention, see *Remote Wipe & Geo-Locate.*
- For BYOD Security Support, see *BYOD Safeguards.*

01 ENCRYPTION / KEY MANAGEMENT

UltraSafe's 3-tier encryption process delivers the highest level of backup data security available: 256-bit AES encryption in CBC mode. Data is first encrypted locally, then in transit via SSL, and then at-rest in the cloud. You end up with "zero knowledge" (or "double blind") encryption.

Infrascale uses two forms of encryption for your data: at-rest encryption (128-bit block size) and UltraSafe encryption (256-bit block size). We can employ both simultaneously.

At-rest encryption uses the following algorithms:

i. The initialization vector (IV) is derived using a custom algorithm that converts a user's numerical ID into an obfuscated payload (non-numeric) thousands of characters long.

ii. This is a 4-stage operation, each stage providing a hash of the payload's current form that is then used to provide a portion of the IV.

iii. The result is a 16-byte (128-bit) IV consisting of binary data (i.e., it's not simply alphanumeric, and is unique for each user).

iv. The at-rest encryption key is derived in a similar fashion: creating a large obfuscated payload thousands of characters long from the user's numerical ID, and hashing it in stages to produce a final key.

v The payload hashes are also salted with a "shared secret" unique to each private cloud instance.

vi The final result is a 32-byte (256-bit) encryption key consisting of binary data that is unique to the user.

At-rest encryption is solely server-side, and is transparent to the end user. Since the keys are derived via an algorithm, there's no need to store encryption keys on disk or in the database – you just can't copy or "find" them amongst the site data.

UltraSafe encryption uses the user's password and a salt to derive its encryption key, which remains client-side. Its keys are never sent to our servers.

With UltraSafe, nobody but the account holder has the keys to unlock stored data. It means that Infrascale cannot access/decrypt data stored on its cloud. When it's time to delete it, secure multi-pass delete will destroy the data permanently.

The operators of most cloud services have the ability to access data stored in their system. UltraSafe means that Infrascale does not.

02 ACCESS CONTROLS, MONITORING, AUDIT TRAILS

The UltraSafe system provides multiple levels of access controls to various role types (Administrator, User, etc.). All global Infrascale infrastructures are monitored by a 24x7 administrative team, including security personnel.

All system access events are logged and audit trails kept. Access controls extend to allowing administrators to control individual device authorization.

The approval process is also tied to a browser instance in combination with an IP address. Two examples of this kind of control:

- Administrators can set a rule which says Joe's computer can connect, but Joe's iPhone can't.
- Jane's IE login works, but she must login separately if she switches to using Chrome.

Strong passwords are enforced. They must be – with UltraSafe encryption, the password is used to derive the encryption key!

- On the first device accessing the Infrascale cloud, the user enters a new password.
- On any subsequent device, the user must enter the password again.
- The password is stored (encrypted) on disk, using a machine-dependent key.
- The resulting configuration file cannot be transferred from one machine to another. UltraSafe will reject any such attempt.

03 DEPLOYMENT FLEXIBILITY

Choose which network you want your data on! Our customers want options for their deployments. So we offer our software platform on a "your cloud, our cloud or any cloud" deployment model – customers can run Infrascale in their own private cloud, leverage our SaaS offering, or install Infrascale software on their public cloud of choice (e.g., Azure or AWS).

You choose the hosting environment that meets your security standards.

04 SECURED INFRASTRUCTURE

We partner with IBM for our backend cloud facilities, and work with them to lock down security at the network and physical layers. We use Tier 3- and Tier 4-grade data centers. The entire Infrascale backup solution is HIPAA, PCI and Sarbox compliant. Datacenters are SAS70 II and SSAE16 certified.

Dedicated intrusion detection and prevention devices are in place, in conjunction with Cisco firewalls. We run regular penetration tests and security audits on each infrastructure level.

Facilities are staffed and secured with video surveillance 24x7. Biometric access controls limit physical access to datacenter floors. All servers are security-hardened prior to deployment. IBM also performs regular virus scanning, system patching, and security profile reviews.

All five essential stages of security, covered by UltraSafe. But by adding Infrascale's EndGuard endpoint data protection, you can protect two mobile security fields: Mobile Data Leaks and BYOD Security Risks.

05 REMOTE WIPE & GEO-LOCATE

EndGuard adds more advanced security features targeted at preventing data leaks and stopping data loss. Find any device with Geo-Location, and wipe it with Remote Wipe (selective data wiping, or a complete drive format)—right from the Infrascale Dashboard.

06 BYOD SAFEGUARDS

Deploy EndGuard on BYOD devices. It protects only the corporate data homed on those devices, taking care of backups without any user involvement needed.

Plus, the Selective Wipe feature keeps your protection when an employee leaves. Even on a BYOD device, corporate can still be wiped at a click. Stopping data loss AND theft in its tracks.

Data privacy in the cloud is no longer a problem with Infrascale's UltraSafe.