

## hetras Whitepaper

# Security

Keith Gruen, keith.gruen@hetras.com  
February 2010

## Introduction

hetras provides state-of-the-art security to ensure that your data is never compromised. At hetras, we know that security is crucial to you – that's why security is our top priority. We devote significant resources to continually develop our security infrastructure. The result: unsurpassed security and privacy for our customers' information. With hetras, you enjoy protection and peace of mind that only our first-class security infrastructure can provide.

We provide a layered approach to securing your data:

- Infrastructure Security
- Operating Security
- Application Security

These layers provide multiple barriers against attempts to breach our security. In addition, hetras utilizes the most up-to-date anti-virus-scanning technology to ensure that your data remains virus-free and increase service continuity.

## Infrastructure Security

### *Physical Security*

Our production equipment is collocated in [IP Exchange, Munich, Germany](#) at a data center that provides 24-hour physical security, manned security checkpoints, redundant electrical generators, redundant data center air conditioners, and other backup equipment designed to keep servers continually up and running. Internet connection is redundantly provided by multiple major carriers.

### *Perimeter Defense*

The network perimeter is protected by multiple firewalls sourced from an industry-leading security vendor. In addition, hetras monitors and analyzes firewall logs to proactively identify security threats. hetras also contracts with a third-party security firm that proactively monitors our security configurations for changes, vulnerabilities, and errors and regularly conducts vulnerability threat assessments including penetration tests.

### *Data Encryption*

hetras leverages the strongest encryption products to protect customer data and communications, including 256-bit [DigiCert SSL certification](#).

## Operating Security

### *Operating System Security*

hetras enforces tight operating system-level security by using a minimal number of access points to all production servers. We protect all operating system accounts by enforcing public-key

## staying ahead

---

cryptology based on SSH-2 to authenticate the remote computer and user. All operating systems are maintained at each vendor's recommended patch levels for security and are hardened by disabling and/or removing any unnecessary users, protocols, and processes.

### *Server Management Security*

All data entered into the hetras application by a customer is owned by that customer. hetras employees do not have direct access to the production equipment, except where necessary for system management, maintenance, monitoring, and backups.

### *Reliability and Backup*

All networking components, load balancers, Web servers, and application servers are configured in a redundant configuration. All customer data is stored in a database served by a database server cluster for redundancy. All customer data is stored on carrier-class disk storage using RAID disks and multiple data paths. All customer data, up to the last committed transaction, is automatically backed up to a primary backup server on a nightly basis.

## Application Security

### *User Authentication*

Users access hetras only with a valid username and password combination, which is encrypted via SSL while in transmission. Users are prevented from choosing weak or obvious passwords: There have to be at least eight characters including at least one special character and one digit. An encrypted session ID cookie is used to uniquely identify each user. Users are forced to change passwords after a specified number of days.

### *User Authorization*

Our fine-grained and robust application security model ensures that users can only access and do what they are allowed to. It is possible to limit functionality as well as access to specific hotels, reports or other data subsets. This security model is reapplied with every request and enforced for the entire duration of a user session.

### *Separation of Hotels and Hotel Chains*

hetras follows a tiered multi-tenant concept of hotel data. Each hotel or group of hotels can be contained in a virtual database providing addition security and separation from other hotel data. If desired, tenants can be stored on separate physical database servers, further enhancing security.

## Virus Protection

hetras uses CA Threat Manager for the Enterprise, one of the most comprehensive anti-virus engines, to protect the system. All uploaded documents and incoming attachments are scanned. The virus definition database is updated automatically on a real-time basis.

## Redundant Data Center

As hetras expands its customer base in other continents, we will consider opening synchronized data centers in other continents as well. This will improve latency and performance around the globe as well make the hetras data truly disaster-proof.