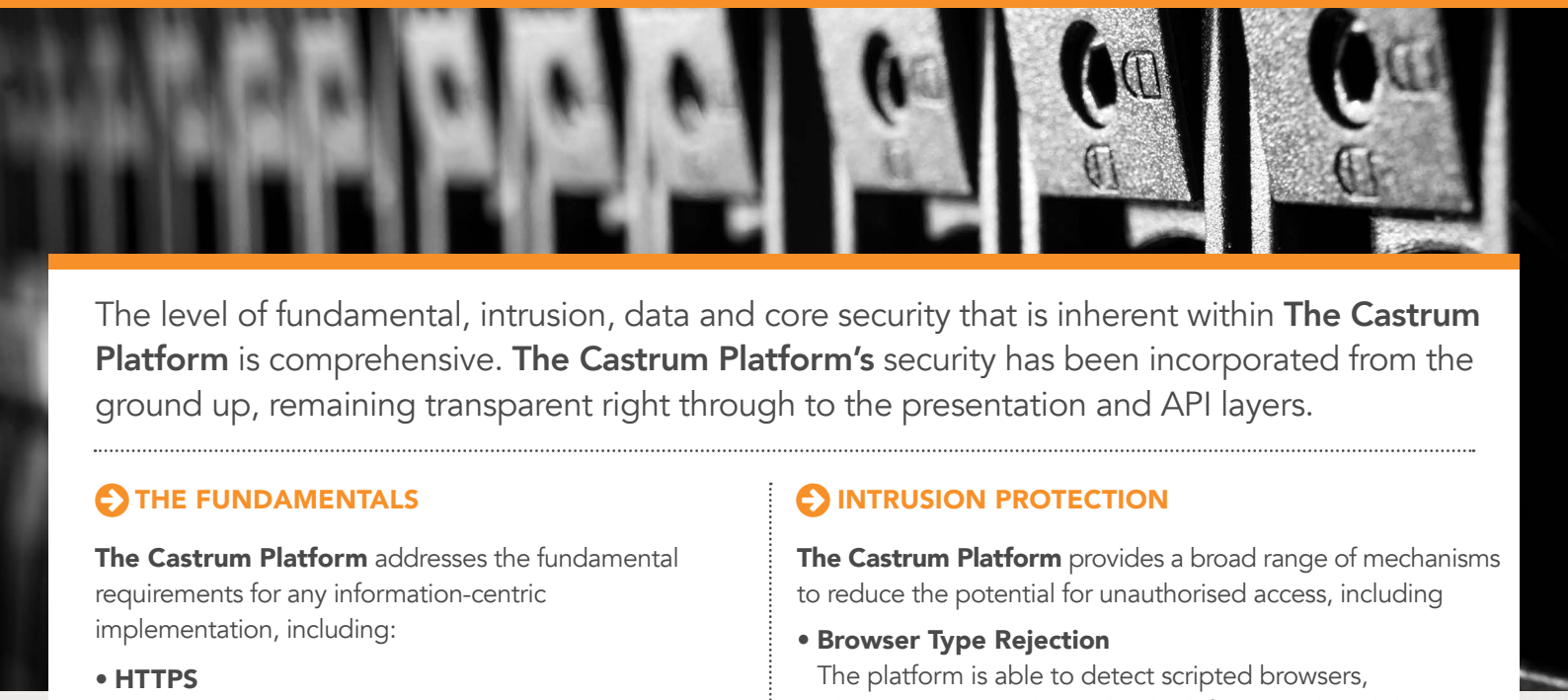
castrum
simple. smart. secure.

# SECURITY OVERVIEW



The level of fundamental, intrusion, data and core security that is inherent within **The Castrum Platform** is comprehensive. **The Castrum Platform's** security has been incorporated from the ground up, remaining transparent right through to the presentation and API layers.

## THE FUNDAMENTALS

**The Castrum Platform** addresses the fundamental requirements for any information-centric implementation, including:

- **HTTPS**
  All data transfer into and out of the platform is via 256-bit SSL *(Secure Socket Layer)* using an encrypted token.
- **IP Range Lockdown**
  The platform can be locked down to allow connections only from specific IP ranges. This serves to frustrate potential attacks, particularly when used in conjunction with other appropriate security features.
- **Strong Password Policy**
  The platform operates a fully configurable password policy, which prevents weak password creation, based on a series of pre-defined criteria.
- **Forced Delay For Incorrect Login**
  Automated username and password attacks, including dictionary attacks, are effectively frustrated by the platform's ability to increase the delay between subsequent failed login attempts.
- **Dual-Factor Authentication**
  2-FA adds an extra layer of security to services by requiring all users to establish their credentials before they can sign-in. It is the simplest and most effective way of achieving enhanced password protection in preventing unauthorised access to confidential information. Password and a Security PIN sent to the user on sign-in. PIN codes are valid for a limited timeframe and automatically expire.

## INTRUSION PROTECTION

**The Castrum Platform** provides a broad range of mechanisms to reduce the potential for unauthorised access, including

- **Browser Type Rejection**
  The platform is able to detect scripted browsers, which are commonly used to look for site vulnerabilities, and reject access accordingly.
- **Tamper Proof Audit**
  The platform maintains a secure, encrypted audit trail of every data transaction within the database, including user access and entity-level activity. The inherent encryption of this audit trail makes it effectively tamper-proof.
- **Identity Spoof Elimination**
  During any session, the security token sent to the client is encrypted to encapsulate both the IP address and the session ID. These two entities must match, when validated at the endpoint, otherwise the session is terminated. This technique provides protection against *"man in the middle"* identity spoof attacks.
- **URL Discovery Protection**
  URL discovery, or vectoring, is a technique whereby an attacker will attempt to substitute all or part of a known URL for some new information, in order to try and gain access to associated information that might require elevated privileges. The platform protects against this by enforcing strict Access Control Lists (ACLs) on every individual resource.
- **SQL Injection & Cross Site Scripting Detection**
  The platform renders both SQL injection and javascript injection attacks harmless by using parameterised data calls into the secure database. This technique effectively checks and sanitises inputs before they reach the database, in order to strip out potentially threatening content.

**CASTRUM** Unit 3 New Fields, Stinsford Road, Poole, Dorset BH17 0NF
01202 835300 info@castrum.co.uk www.castrum.co.uk
Connect with us:

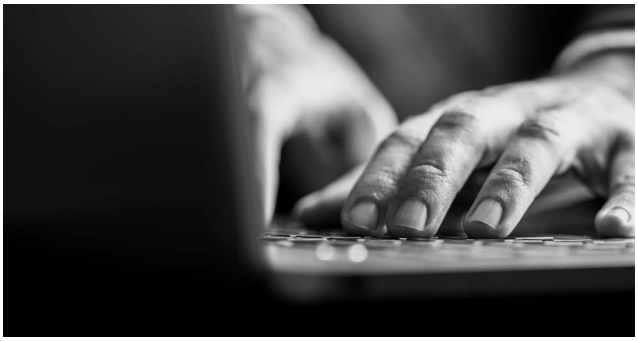
castrum
simple. smart. secure.

# SECURITY OVERVIEW (CONTINUED)

## DATA PROTECTION

**The Castrum Platform** vigorously protects internal data via a number of superior grade security features including:

- **Access Checking**
  The platform provides for true access checking and verification at information level as opposed to the more usual folder level.
- **Continuous Encryption**
  Encryption within the confines of the platform is continuous and complete, such that captured documents never exist in an unencrypted state, even during potential intermediate storage scenarios such as when scanning direct into the platform.
- **Information Encryption**
  All information held within the platform is encrypted using the *Advanced Encryption Standard (AES)*, further enhanced by recursion, salting and other measures unique to Castrum. Furthermore, since all information is held within the database itself, rather than making use of the underlying file system and associated filenames, this in itself ensures significantly less vulnerability to attack.
- **Information Fingerprinting**
  SHA hashing is used to digitally fingerprint each and every individual item of information held within the platform, thereby protecting against unauthorised information changes or swaps, in addition to just content modification of in-place data.



## CORE PROTECTION

**The Castrum Platform** is incredibly flexible by virtue of its extensibility, however the core remains protected via:

- **Plugin Fingerprinting**
  In a similar fashion to information fingerprinting, SHA hashing is extended within the platform to cover core plugins. These are modules which add huge flexibility by extending the platform capabilities, but which clearly need to be viewed with scrutiny by the core. Fingerprinting ensures that malicious plugins cannot be easily introduced.

## THE CASTRUM HOSTING CENTRE

Castrum hosted solutions are deployed within our secure hosting centre. This has been specified to meet the very highest level of requirements, including:

- Information Security Management accreditation to *ISO 27001:2005* standard
- Industry leading *Fire Suppression Systems*
- *Proximity Card Reader Access Control*
- 24-hour On-site Security
- 24-hour Video Surveillance
- Complete *N+1 Redundancy*
- Three separate *National Power Grid Feeds*
- Climate Control Systems
- Multiple *UPS Systems* and *Backup Power Generators*
- Inherent anti-virus/operating system hardening

Additionally, our chosen firewall architecture is EAL4+ compliant and integrates multiple security features including network fire-walling, network intrusion detection and prevention, denial of service and gateway anti-virus.