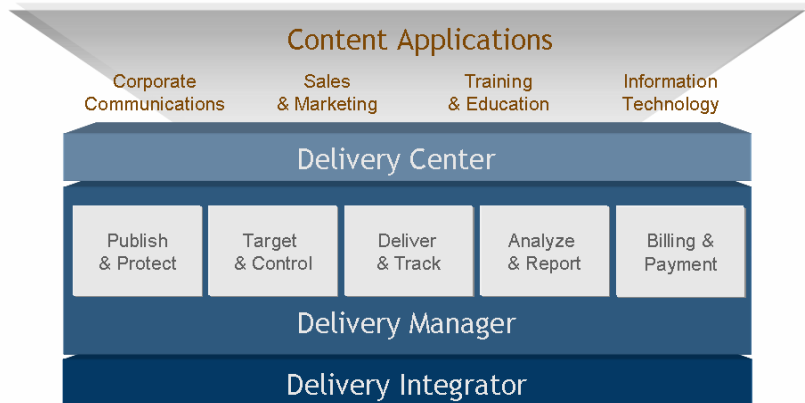


Ignite provides the industry's most secure and scalable Content Delivery Solution, enabling customers to efficiently publish, deliver, and manage digital assets – from rich media content for training and communications to software patches and virus updates – to anyone, anywhere, at any time. Ignite's patented Content Delivery Solution overcomes network and connectivity constraints that have limited the ability to reach online audiences with the highest quality, secure rich media. Ignite's Solution has been deployed around the globe at companies like Accenture, BearingPoint, Sabre, and Proctor & Gamble.



Ignite's World-Class Security Infrastructure

Security is always a major concern when it comes to distributing digital content. You want your content to be fully protected throughout its entire lifecycle – from publishing and targeting through delivery, receipt, and use. Ignite incorporates multiple layers of physical, user, and content security to ensure that your critical content is never compromised. Physical security provides protection against intruders and ensures the system will tolerate failures. User security ensures that only authorized users can receive and view content and allows you to assign specific rights to individual Administrators or groups of Administrators. Content security controls how content is protected throughout its lifecycle. These security measures can be customized to meet your unique needs.

Ignite devotes significant resources to continually enhancing its world-class security infrastructure. The result is unsurpassed security for your content.

Physical Security

Ignite's computing environment uses the most sophisticated security technologies available. The entire server platform is protected by fully redundant firewalls, network switches, and cross-connections that are configured to provide automatic fail-over capabilities in case of a malfunction at any given point. In addition, an intrusion detection system (IDS) is constantly updated with the latest attack and intrusion signatures.

This system automatically blocks malicious attacks to the site, generating administrative alerts and notifications based on intrusion attempts.

Each server is protected by share level and New Technology File System (NTFS) level security. Each system allows only specific accounts to authenticate, and their events are logged. The database cluster is located on a different subnet, physically separated from the application system by yet another set of firewalls. Only specific hosts at specified ports are allowed to access the database cluster.

The access network is protected by access control lists (ACLs) that allow only specific IP addresses to communicate within the predefined subnet. All remote connections to the site are through a VPN, using industry-standard, Triple-DES encryption. Multiple server farms are used to eliminate single points of failure. This creates a highly secure, highly available, and predictable performance-oriented environment, designed specifically to deliver large amounts of data to globally dispersed audiences.

User Security

Ignite provides for various levels of user roles and responsibilities, as well as corresponding rights and privileges. User security ensures that only authorized users can receive and view content and allows you to assign specific rights to individual Administrators or groups of Administrators. Following are the primary user

security components, which can be customized as needed.

Administrative User Authentication

A key feature of the Ignite system is its fully integrated, centralized Delivery Manager application for the administration of all system functions. It is vital to ensure that only legitimate authorized users have access to sensitive information as well as to protect transactions and data from unauthorized tampering or redistribution.

Each Ignite customer has its own Ignite Content Delivery Solution database instance. Within a company, one or more Administrators can be given access to the Delivery Manager to perform specific tasks. Delivery Manager access is secured through a variety of mechanisms, as described below.

Accessing the Delivery Manager requires a unique URL and a company code specific to the company. Each Administrator is given a unique username and password which must be used to login to the Delivery Manager.

Ignite customers can also choose to apply the following additional security measures to enhance their Administrative user security.

IP Address Restrictions

Access to the Delivery Manager can be restricted to specific IP addresses or IP address ranges.

Digital Certificates

To enhance the authentication process, the Delivery Manager can be configured to require digital certificates for user login. Each Administrator can be issued a unique digital certificate. Whenever the Administrator attempts to access the Delivery Manager, authentication is performed based on this digital certificate. Digital certificates are computer-specific, so an Administrator can login only from an authorized computer.

To ensure the highest standards of security, Ignite has implemented X.509 digital certificate technology with the following integration options:

- **VeriSign's Digital ID** – VeriSign is the leading provider of digital trust services and the worldwide de facto standard in digital security. Ignite combines VeriSign's industry-standard technologies with its own digital communications technology to provide an authenticated, private, and non-repudiable system.

- **Other Digital ID Providers** – Other vendors, such as EnTrust and GTE, provide standards-based digital ID services similar to VeriSign's. Ignite can use existing standards and protocols specified by those providers to integrate with their services.
- **Ignite's Digital ID** – Ignite provides its customers with its own X.509 capabilities to give you the same non-repudiation authentication features as VeriSign and other vendors. Ignite's digital IDs are offered at a substantial operational cost savings.
- **Existing Public Key Infrastructure (PKI)** – Ignite's support for administrative user authentication standards allows the Ignite system to easily integrate into your existing PKI infrastructure. This enables you to set certificate revocation standards and timeliness according to your own specifications.

End User Authentication

End user authentication includes:

- Registering and authenticating an end user for the purpose of receiving and accessing content via the Ignite system
- Ensuring ongoing validity of user identification for content delivery and use

Before or during the deployment of Ignite's system, company-designated end user identification, such as email address, employee ID, domain login ID, or other unique identifier(s) as determined by the company, is provided to the Ignite system via data export or via Ignite's Directory List Synchronization (DLS) facility. Ignite's DLS is a highly modular synchronization utility that can easily be integrated into existing user management systems via open standards-based protocols such as SOAP, SML, LDAP, HTTP, and others. Upon deployment, the end user's unique ID is authenticated against either existing company authentication systems (such as Active Directory, PKI (X.509) Infrastructure or RSA SecurID) or company-provided information to validate and enable receipt and use of content. Once authenticated, Ignite generates and stores that user's encrypted identity (known only to Ignite) on the user's computer. Prior to and during all communications, the encrypted identity is verified between the Ignite client application and the Ignite servers to maintain security and control.

Administrative User Rights

Ignite's content publishing and distribution process is made up of six distinct steps: Encrypt, Sign, Publish, Approve Content, Target, and Approve Distribution. The Ignite Security module provides for the separation of any combination of these steps to provide a highly-customizable, secure, and auditable content publishing, control, and approval process.

Delivery Manager Access

Administrators can be granted rights to access specific Delivery Manager modules and to control the behavior and execution of content, such as setting execution, expiration, and download availability dates. They can also be given rights to control the customizable aspects of Ignite's content security process, such as applying Ignite encryption to content and selecting end user authentication attributes.

In addition, role-based administrative settings allow Administrators to be given rights to specific functions or groups of functions, such as Publishing, Targeting, Reporting, etc. Restrictions can also be placed on the types of packages and end users with which an Administrator can interact. For example, an Administrator in the marketing group could be granted access only to marketing users and only be able to deal with marketing content.

Checks and Balances

Because Ignite's content publishing and distribution process is broken into these separate steps, you can set up access controls at a very granular level for individual Administrators or groups of Administrators. For example, if you have multiple Administrators, you can set up a scenario where:

- Administrator 1 uploads and publishes the content package into the system.
- Administrator 2 tests and approves the package for distribution.
- Administrator 3 sets a targeting event which generates a list of users to whom the package should be targeted. Targeting criteria can be based on one or more of the many data points that are already in the system.
- Administrator 4 approves the target list for this particular delivery.

After the entire process is complete, the content will begin delivery to the intended end users.

Chain of Custody Control

Another important aspect of Ignite's security is the auditable chain of custody that is created for all content that passes through the Ignite system. Ignite tracks the digitally-verified identity of every user who handles the content for any of the content publishing and distribution steps. This allows for a documented chain of custody for every delivery and transaction made through the Ignite system.

Auditing and other reporting is available via the Ignite Delivery Manager or it can be integrated into other operational consoles via standards-based interface techniques using SOAP, XML, HTTP and other protocols, depending on your requirements.

Content Security

Ignite's multi-layered approach to content security provides the most comprehensive and secure solution available. Ignite's multiple security barriers safeguard your critical assets and make unauthorized capturing, viewing, duplicating, or altering of content virtually impossible. This methodology protects your digital assets during all phases of delivery, viewing, and user management.

Ignite's multi-layered security uses a modular approach that provides for seamless integration with industry-standard and customer-provided digital rights management, encryption, digital signature, and secure token applications.

By incorporating Ignite proprietary technology along with industry standards from Microsoft, Adobe, BackWeb, VeriSign, and RSA, Ignite offers the most secure content delivery platform available.

Virus Scanning

During the publishing stage, content is uploaded to a sequestered area on the content server, where two anti-virus scans are performed. The virus definitions for both of these scanning programs are updated at least once daily. If no problem is detected during these scans, content is moved from the sequestered area to a pre-publish directory so the Administrator can continue with the publishing process. If a problem is detected, the content is deleted and the Administrator is alerted.

Digital Rights Management (DRM)

A set of rules is encrypted into every content delivery to allow the Ignite system to enforce digital rights management. Ignite provides a unique combination of proprietary digital rights controls that can be used standalone or seamlessly integrated with industry-standard applications.

Third-Party DRM Integration

Ignite fully supports existing DRM-enabled products such as Microsoft Windows Media DRM, BackWeb DRM, and Adobe Acrobat's DRM solutions. In addition, customer-provided DRM applications can also be incorporated for use with the Ignite system. By implementing these third-party applications, Ignite provides for the delivery and control of existing digital content and content created with a customer's previously-determined DRM rules.

Overcoming Limitations

Standard DRM solutions are limited because they typically apply only to content in specific formats. Most other native electronic data formats, such as non-Microsoft video files, word processing applications, graphics presentations, and web pages, are inherently insecure because they do not provide for digital rights management. To overcome these limitations, Ignite's technology incorporates certificates and token-based security and authentication modules from VeriSign and RSA to provide extremely sophisticated and comprehensive DRM capabilities. These capabilities enable the Ignite system to extend security to a wider variety of content and additional operating systems. For example, Ignite supports Windows 95 and Windows NT, while many third-party DRM applications and other content delivery platforms do not.

Control Attributes

Ignite's integrated DRM provides customizable rules that set various properties for each piece of content to govern and control the recipient's access and use. These rules include:

- **Expiration Date** – The sender can specify an exact date and time that the content will become unavailable and automatically delete itself from the recipient's hard drive.
- **View Date** – The sender can specify an exact date and time that the content will make itself available to the recipient, even though it may have been delivered days or weeks prior to the view date. This allows the sender to create, stage, and deliver content in advance and set the content to become available to be displayed simultaneously for all recipients.
- **View Number** – The sender can specify a precise number of views the recipient is allowed before the content becomes unavailable and automatically deletes itself from the recipient's hard drive.
- **Prevent Re-Distribution** – Ignite prevents users from re-distributing or saving secured content. For example, a secured video can only be played on authorized Delivery Centers. Attempting to copy a video and play it outside the Delivery Center renders it unusable.

Encryption

Encryption is a process that uses a conversion algorithm to change sensitive data into coded form. The coded version of the content is distributed, and it can only be reconverted or decrypted to its original state by authorized users (i.e., users who have knowledge of the description process and the decryption key).

Ignite uses a variety of encryption methods, starting with a base of 128-bit encryption. This base encryption is based on the industry standard and widely-accepted Advanced Encryption Standard (AES) symmetric encryption algorithm.

Content is encrypted at all times, even as it resides on or is viewed on the client's computer.

Digital Signatures

A digital signature is a form of encryption that ensures that the protected content has not been altered since it was signed, providing assurance that the content data integrity is maintained. It is mandatory that all content published in the Ignite Content Delivery Solution be digitally signed using X.509v3 certificates. All Ignite clients are configured to automatically reject any content with missing or invalid digital signatures.

The publisher of the content also has the option of applying an additional digital signature of his own to provide a multi-layered tamper detection system.

Additional security options include:

Package Security – Administrators have the flexibility to select any of the following security options to apply to a given content package:

- Symmetric encryption using Ignite's default symmetric key (unique for every customer)
- Symmetric encryption using customer-specified key
- Asymmetric encryption using customer-provided X.509 certificate
- Digital signature using customer-provided X.509 certificate

In addition, all packages are digitally signed by Ignite's customer-specific X.509 certificate for performing authenticity checks of delivered content.

Package Publishing – Administrators can secure content packages in one of two ways:

- By using an Ignite-provided standalone utility prior to publishing, or
- By using an ActiveX control during the Delivery Manager's package publishing process

In either case, Administrators can secure the package content outside of and prior to introduction into the Ignite content server by using customer-provided or customer-obtained certificates and keys. The certificate used for encryption and/or digital signing may be any X509v3 certificate, provided the selected certificate can support the functions for which it is being used. The certificates and custom symmetric keys are package specific. The Administrator can choose to use a completely different set of certificates and keys for each package while Ignite's customer-specific symmetric key is common to all packages in the system.

Key Management and Recycling – The Delivery Center supports a private encrypted certificate and key repository for storing customer-chosen certificates and Ignite's customer-specific symmetric key. Administrators can use the certificate update package template to add to or update the Delivery Center's private store with customer-chosen certificates.

Content Parsing

As part of the content delivery process, the Ignite server fragments the content into many tiny packets so that it appears as normal network traffic and does not clog network resources. Therefore, during the data transmission, the content is transferred not as a single file, but as many small packets that are individually meaningless until they are reassembled on the client's computer by the Ignite client software. Ignite's encryption techniques and digital signatures render any subset of the content inaccessible, even with the proper decryption keys.

Content Access Security

The last step in the Ignite content security process is to ensure that the content can only be accessed by the appropriate recipient(s). Content security is performed by the Delivery Center rather than the native content viewer (e.g., Windows Media Player), allowing the Delivery Center to carry out all necessary security checks in a secured and extensible manner.

The Delivery Center executes the following security validation steps:

1. Check DRM rules (mandatory)
2. Revalidate all content files (optional)
3. Apply Ignite decryption (optional)
4. Execute content

Malicious content cannot be introduced into the Delivery Center by the end user because the Delivery Center checks to ensure that content was delivered through the Ignite CDS before allowing any interactions. This check and the other security options mentioned above provide the necessary authentication and authorization for content access.

The architecture for the Delivery Center's content access security process is built to be easily extensible. For example, the content access security process can be extended to leverage rights management implementations, security processes, and directory services checks currently being used by a customer.

Summary

Ignite's multiple layers of security provide optimum protection for your sensitive content. Physical security provides protection against intruders and ensures the system will continue to operate in the event of a malfunction. User security ensures that only authorized users can receive and view content and allows you to assign specific rights to individual Administrators or groups of Administrators. Content security controls how content is protected throughout its lifecycle. These security measures can be customized to meet your unique needs.

To experience Ignite's Content Delivery Solution firsthand, visit Ignite's website at www.ignitetech.com and click on the "Experience Ignite" link.

The Ignite Difference

Multi-Layer Security

Ignite's physical, user, and content security ensures your critical content is never compromised.

Customizable Security Controls

Select from various digital ID options, assign Administrative rights, and set up checks and balances and chain of custody control.

Full Lifecycle Security

Unlike other content delivery solutions, Ignite keeps content secured throughout its entire lifecycle.

Comprehensive Digital Signature Protection

All content delivered by Ignite is digitally signed, and all Delivery Centers are configured to reject any content that has a missing or invalid Ignite digital signature.

Support for Extensible Security

If Ignite customers have their own security mechanisms, such as directory services security or legacy encryption software, the Delivery Center and Delivery Manager can easily integrate with these mechanisms.