

Digital Asset Security Within the Castle Walls

By Mike Urbonas, Director of Product Marketing, Nuxeo



Michael Urbonas

Michael Urbonas, director of product marketing at Nuxeo, has over 15 years of software marketing experience that spans ECM/DAM, enterprise search, text analytics, business intelligence/data warehousing, and ERP.

Organizations recognize digital asset management (DAM) as a key strategic investment to maximize the business value of digital media and other content. Digital Clarity Group executive Cathy McKnight recently remarked that “*while content remains king, building a proper castle in which these royal assets will live is becoming more important.*”⁽¹⁾

The castle analogy also aptly describes much of the security elements your DAM platform must have to fully protect your organization’s invaluable digital assets.

Many technologists mistakenly believe that comparing content security with castles is an outdated analogy focusing only on perimeter security. This is based largely on the false notion that a medieval castle was protected only by its visible fortress walls. In fact, behind their outer walls, castles had intricate networks of *internal* security elements. Invaders getting past the front gate found themselves blocked by inner walls and towers, or even worse, trapped in a gatehouse tunnel with guards firing through holes in the ceiling!

A truly secure DAM platform will also minimize the harm intruders can possibly cause. For example, the Nuxeo Platform for developing, testing, and deploying content-critical applications supports encryption of network traffic with configurable SSL as well as AES encryption of all content at rest (in storage), preventing illicit access to digital assets directly from content storage back ends. It is also possible to encrypt the backend database and search indexes at a system level.

Like content security today, castle security included *authentication protocols* to prevent would-be attackers from tricking guards into opening the front gate. For example, loyal soldiers would carry a flag bearing the lord’s “personal standard”—a unique design guards would recognize and allow entry.

Similarly, digital asset management platforms must support the authentication tools of choice for each organization. For example, the Nuxeo Platform supports a full array of authentication protocols and providers, including login/password, oAuth, SAML2, OpenID, LDAP/AD, Shibboleth and advanced two-factor authentication (2FA). The modular, “API-first” design of the Nuxeo Platform also makes it easy to write a plugin to implement a custom authentication protocol.

Castle security also had to facilitate the day-to-day operations of its many workers—including cooks, bakers, servants, craftsmen—each with rigidly defined responsibilities. Supervisors, or “reeves,” ensured workers performed their work on time and that nothing was stolen; in effect, enforcing the *access controls* of the castle.

“While content remains king, building a proper castle to secure these royal assets is more important than ever.”

Of course, DAM platforms also enforce access controls, using ACLs. However, ACLs alone do not provide adequate enterprise digital asset security. Nuxeo, for example, provides two concurrent layers of security that users **cannot** bypass:

- ◆ **Access control lists (ACLs)** are used by Nuxeo to manage security at the data level. Nuxeo provides the ability to allow administrators to define ACLs via the Nuxeo UI. You can also use code to apply ACLs programmatically.
- ◆ **Custom security policies** consist of dynamic code that will be executed each time the Nuxeo repository needs to determine whether or not to allow a user access request or other user action. Custom security policies enable Nuxeo to enforce mandatory access controls (MACs) that may override or supplement any applicable ACLs—a common requirement for military systems.

These layers of security can be used to **limit user access** (for example, Andrew is permitted to download company advertising images, limited to a low resolution version) as well as **limit user actions** (because Lori does not have permission to modify existing files, the Nuxeo Platform does

not display an “edit” button as part of her application UI).

As any true enterprise content management platform should, Nuxeo provides a comprehensive audit log module to capture and record any system or application event. An event bus is also included that allows the registration of event listeners, which can trigger one or more workflows upon a given event taking place, such as changes in user permissions.

Many lords and ladies lived in more than one castle over the course of a year, with certain valuables stored in each. Somewhat similarly, digital asset management platforms today must be capable of integrating and applying security controls to digital assets wherever they reside, including Amazon S3 and other cloud storage, as well as content delivery networks (CDNs) and enterprise file sync and share (EFSS) platforms such as Google Drive and Dropbox.

The Nuxeo Platform provides this key functionality by storing each binary file separately from its metadata, which is retained in a SQL or NoSQL database. The binary files themselves are natively de-duplicated and stored in any supported file store: local file systems, encrypted FS, Amazon S3, Azure CDN, and many others.

Additionally, *Nuxeo Live Connect* integrates with files residing in Google Drive, Dropbox, Box, and Microsoft OneDrive/OneDrive for Business. Nuxeo manages these files in place while adding full text search, versioning, security, and integration into enterprise workflows, as seamlessly as if the files were stored within the Nuxeo repository.

Far from relying solely on outer walls for protection, castles applied effective security controls that guarded against internal and external threats. By ensuring your digital asset management platform of choice does so as well, you will have a solid foundation on which to build a successful content security strategy that will help minimize security vulnerabilities from happening in the first place. ■

Nuxeo provides an extensible and modular enterprise content management platform that enables software architects and developers to easily build and run business applications. 1.888.882.0969, contact@nuxeo.com, www.nuxeo.com

(1) Cathy McKnight, Digital Asset Management Round-Up, Digital Clarity Group blog (Feb. 18, 2016).