

Maintain Data Security with CAM's Access Management Capabilities

The world is experiencing a rise in cyberattacks as cybercriminals and hackers' prey on potential weak points across organizations' security systems. Following major attacks like SolarWinds, Microsoft Exchange, and LinkedIn, there has never been a better time for your organization to reexamine its security policies.

Many cyberattacks come because of human error. Users unknowingly create cybersecurity risks within the organization by interacting with sketchy email links, saving documents in their vulnerable personal drives, and attempting to access data and projects that are irrelevant to them.

There are also other cases when users intentionally abuse their level of access, especially if their relationship with the organization is coming to an end. Hackers capitalize on these weaknesses and use them to breach vulnerable endpoints and workstations.

While organizations may not always be able to prevent a data incident, they can take measures to ensure that they are protected when it does happen. The key is Privileged Access Management (PAM).

What is Privileged Access Management?

Privileged Access Management is a strategic approach to cybersecurity that centers around monitoring all users and their levels of access across a given workspace. PAM helps organizations apply a structured level of access where users can only access data that is necessary to do their jobs. This not only prevents users from accessing irrelevant data to their position, but the organization can also detect malicious activity and act on it.

This method of security keeps unwanted outsiders out of your data, but also mitigates the risk of a malicious attack from within the organization as well.

As one can imagine, keeping this level of security requires a large number of resources and time when done manually. Sometimes, a software solution is needed to carry your organization to that extra mile.



CAM Privileged Access Management

Mitigating Data Chaos as a Foundation to Privileged Access Management

Constantly monitoring and tracking access levels of all users in the organization is a massive undertaking. It becomes even more challenging when done across collaboration systems, since data tends to be chaotic.

CAM enables provisioning and data protection across collaboration systems. Allowing end users to save data in the right place, providing rich metadata to understand context, and enhancing the risk team's ability to automatically apply privacy and security policies.

Automated Access management

Updating security and permissions for each project is prone to human error and time-consuming. Inappropriate access can result in users breaking compliance policies and client requirements, especially if you are working with external users who have access in Teams. CAM addresses these challenges by enabling automatic access across systems, incorporated with Teams, enabling organizations to set and update security from one platform and apply that to all other collaboration systems.

Re-Certify Access Regularly

Over the lifecycle of a matter, many users will be added or removed as their involvement or roles in the matter changes or ends. Many times, when a user leaves a matter team to work on other projects, their permissions are not removed. To keep up with who needs to view and work on certain projects and when their stint will begin and end, CAM enables organizations to re-certify access permissions regularly. CAM can help audit and report on who has and who needs access to the matters, then help organizations to secure those matters appropriately by adding those who need access and removing those who don't.

The timing and frequency of these check-ins depends on the project/department/organizational needs. This helps cut down on collaboration chaos as well as inappropriate access and helps corporate decide which projects can be closed.

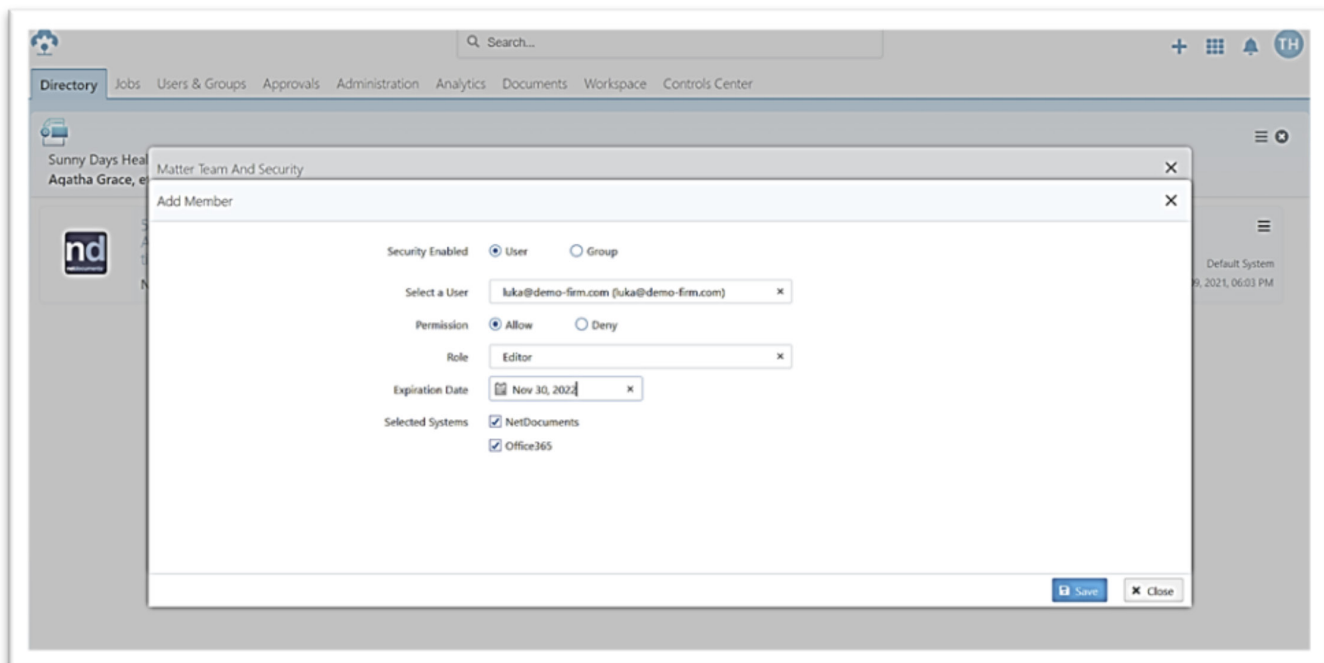
Remove Departed User from Access Control List

When a user leaves an organization or changes departments, CAM ensures that user permissions are removed from every single document they had access to on the organizations Access Control List (ACL) through ISO 27001. Leaving departed users on ACLs for sites, workspaces or documents can open organizations up to further risk. A bad actor might re-able a disabled user's account to gain access to content to which they had access. Removing departed users from ACLs prevents this from happening.

Limited Access on a Project basis

Since employees' responsibilities differ, so should their access to data. With CAM, organizations can limit access to files and data on a need-to-know basis. Users start with the least privileged access and are added to projects as needed. This reduces the number of users that have access to a certain file or matter – in turn limiting the possibility of hackers gaining access or internal users engaging with data inappropriately.

The more limited the access to data is, i.e., on a need-to-know basis, the less the organization is vulnerable to data loss and hacks.

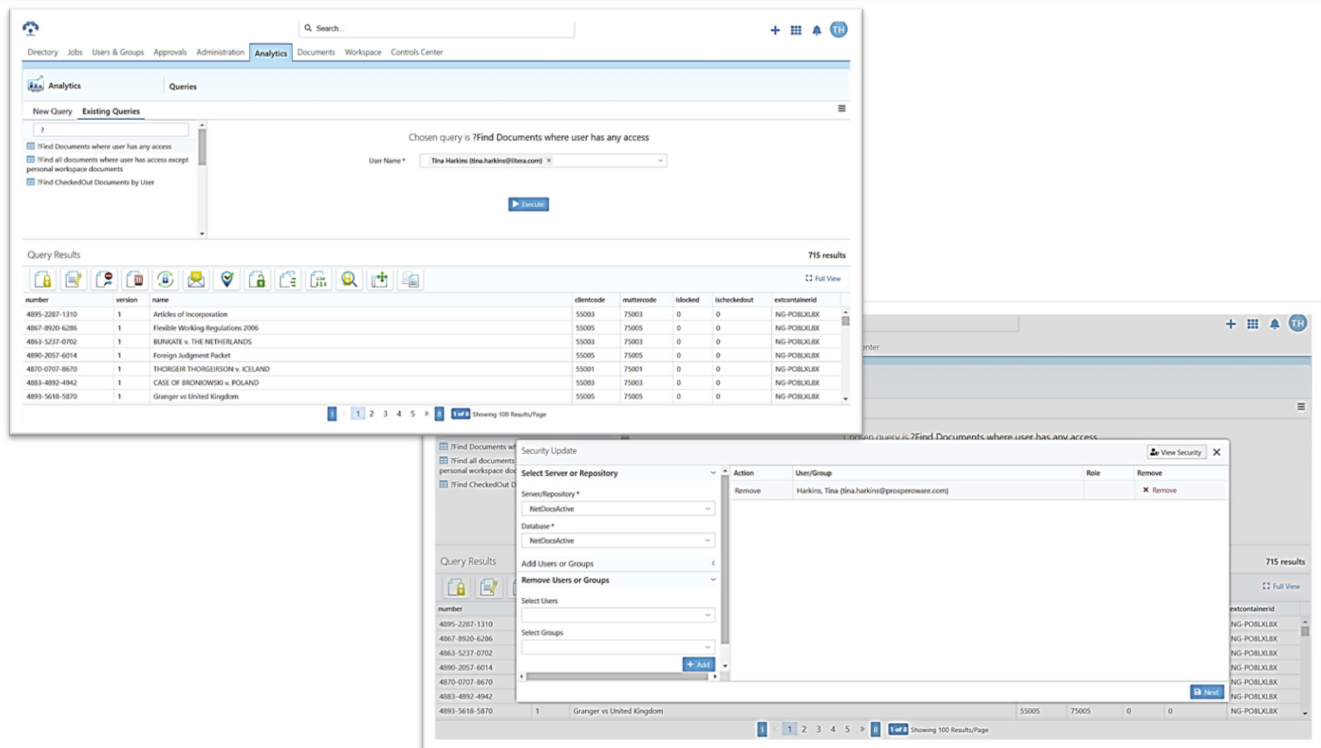


Report on Inappropriate Activity

Considering 90% of data incidents involve human error, organizations need to keep aware of what data their users are accessing, and how they are interacting with it.

With CAM, organizations can run frequent analytics reports to monitor user activity. These reports allow them to monitor activity that appears abnormal, such as users deleting documents, moving files and folders, downloading too many files, and more.

These reports can help your organization figure out if users are unaware of your data protection policies, or worse, intentionally creating cybersecurity risks internally.



The screenshot displays the LITERA Analytics interface. The top navigation bar includes 'Directory', 'Jobs', 'Users & Groups', 'Approvals', 'Administration', 'Analytics', 'Documents', 'Workspace', and 'Controls Center'. The 'Analytics' tab is active, showing a 'Queries' section with a search bar and a dropdown menu. The chosen query is 'Find Documents where user has any access'. Below this, a table displays the query results for the user 'Tina Harkin (tina.harkin@litera.com)'. The table has columns for 'number', 'version', 'name', 'clientcode', 'mattercode', 'islocked', 'ischeckedout', and 'externalid'. The results show several documents, including 'Articles of Incorporation', 'Flexible Working Regulations 2006', and 'BURKATE v. THE NETHERLANDS'.

Overlaid on the bottom right is a 'Security Update' dialog box. It contains a 'Select Server or Repository' dropdown, a 'Database' dropdown, and a table for 'Action' and 'User/Group'. The table shows a 'Remove' action for the user 'Harkin, Tina (tina.harkin@prospectware.com)'. There are also 'Add Users or Groups' and 'Remove Users or Groups' sections with 'Select Users' and 'Select Groups' dropdowns.

number	version	name	clientcode	mattercode	islocked	ischeckedout	externalid
4895-2287-1310	1	Articles of Incorporation	55003	75003	0	0	NG-POBLXLBX
4867-8920-6296	1	Flexible Working Regulations 2006	55005	75005	0	0	NG-POBLXLBX
4863-5237-0702	1	BURKATE v. THE NETHERLANDS	55003	75003	0	0	NG-POBLXLBX
4896-2057-6014	1	Foreign Judgment Packet	55005	75005	0	0	NG-POBLXLBX
4870-0707-8670	1	THORGER THORGERSON v. ICELAND	55001	75001	0	0	NG-POBLXLBX
4883-4892-4942	1	CASE OF BRONONOWSKI v. POLAND	55003	75003	0	0	NG-POBLXLBX
4893-5618-5870	1	Granger vs United Kingdom	55005	75005	0	0	NG-POBLXLBX

If you want to learn more about CAM's Access Management capabilities, [book a demo](#) today and talk to one of our experts.