LITERA

prosperoware

WHITE PAPER

Protect the Data You Need, Minimize What You Don't

THE NEED TO REDUCE RISK AROUND YOUR DATA

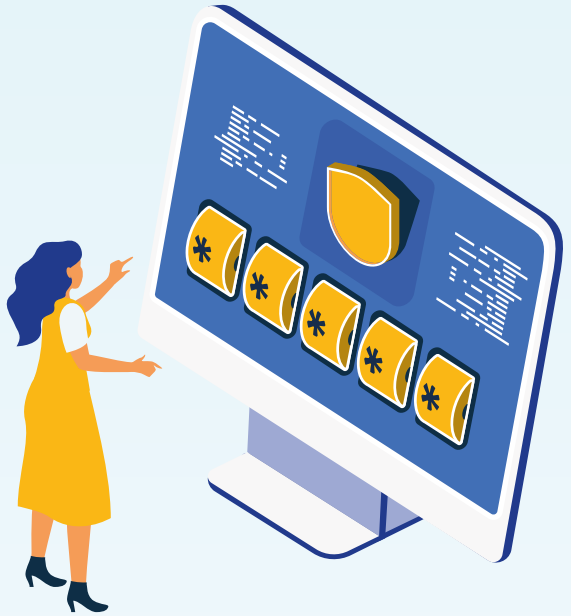
FEBRUARY, 2022

LITERA

prosperoware

Chaos, Risk, and Ransomware

A recent White House memo declared that ransomware – and other forms of cyberattacks – are now on par with terrorism in the eyes of the United States. This document has been a wake-up call for organizations worldwide, sending one simple, but important message: take data protection seriously, or risk losing everything.

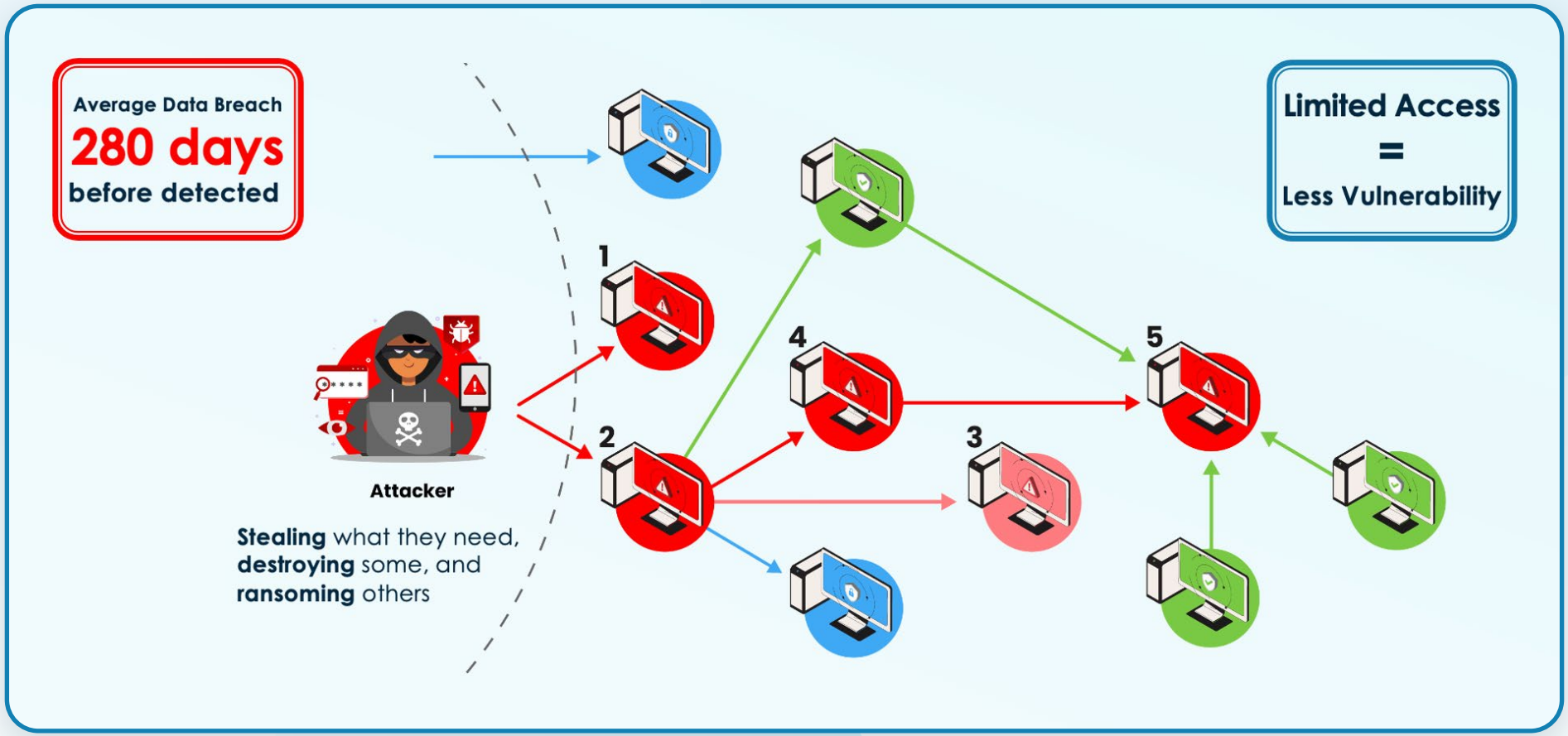


Over the past year, ransomware attacks have increased by over 60%. Cybercriminals have a number of methods they use to breach systems, but one of the most common are phishing emails. This type of attack relies on user error, which is responsible for nearly 84% of data incidents, in order to gain access to passwords and credentials. By stealing user passwords through phishing emails, hackers can interact with all of the files, documents, and data that an afflicted user had access to across an organization's collaboration systems. From there, hackers can encrypt, copy, delete, and even hold files for ransom. What's worse is that this can go on for an average of 280 days until the breach has been detected and contained.

Phishing emails are just one of the tactics implemented by hackers. When combined with the fact that 94% of organizations have suffered insider data breaches, the amount of vulnerabilities and risks within your systems can be far greater than you would imagine.

It is crucial that your organization creates a data protection plan, or risk becoming the next high-profile data breach alongside the growing list of organizations, such as SolarWinds, T-Mobile, LinkedIn, and Colonial Pipeline.

In this white paper, we are presenting a seven-step data protection plan to ensure that in the event of a breach, your organization can maintain business continuity and safely collaborate across systems while reducing risks related to privacy and cybersecurity.



The 7-Step Data Protection and Minimization Method

1 Remove Departed Users from the Access Control List (not natively possible with any system)

What happens to a user's access permissions when their role on a project or matter comes to an end? What about when users leave an organization completely? Unless this user has permissions removed from the organization's Access Control List (ACL), their access to certain projects or matters, still remains.

If a hacker uses a social engineering hack, they can get the organization's Service Deck to re-enable the account and permissions of the departed user. This hacker would then gain access to all files, matters, and data that the user had access to as well.

To remedy this issue, organizations should regularly update their ACL and remove users that no longer require access to certain data, or when a project has been completed. Organizations can do this through ISO 27001 and remove the user from every single document they had access to on the ACL.

Not only does this limit the amount of data a hacker would potentially have access to in the event of a breach, but it also ensures easier data location, since users will have fewer files to go through when looking for a certain document.

Unfortunately, this ability isn't currently native to Microsoft Teams or any other virtual collaboration system, so a third-party solution is necessary.

2 Limit Access on a Need-to-Know Basis

In order to reduce risk and cut down on data chaos, need-to-know security should be the standard.

Since employees' responsibilities differ, so should their access to data. Consider a scenario where your accountant has the same level of access as a system administrator. If hackers compromised the accountants' systems, they would use it as a central point to make their way into other systems, in which they would be able to view, copy, and delete any file. If this is your organization, then you are welcoming a data breach into your system.

Organizations can begin by limiting access to files and data on a need-to-know basis. Similar to the National Institute of Standards and Technology's Zero-Trust model, users start with the least privilege 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. It also prevents users from inappropriately accessing files that are irrelevant to their job, or even carrying out malicious activity like file deletion and copying.

3 Re-Certify Access Regularly

Over the lifecycle of a matter or project, many users will be added or removed as their roles begin and end. Many times, these permissions don't get removed. To keep up with who needs to view and work on certain projects and when their stint will begin and end, organizations must regularly re-certify access permissions. Organizations can send a list of permissions to admins or managers to determine who still needs access and who can be removed.

Once all users have reported they no longer need access to a certain project, that likely means it has been completed. The frequency of these regular checks will depend on both, the number of matters and projects an organization is undertaking, as well as the size of the organization. For example, a large organization with hundreds of ongoing matters or projects will need to re-certify access more frequently.

The recertification process reduces data chaos and cybersecurity risks, by limiting the possibility of unnecessary access of users to data across systems. While also informing organizations on which matters or projects can be closed and which are still ongoing.

4 Dispose of Unnecessary Data

Traditionally, data minimization has been viewed as a "nice-to-have" approach to data protection. Today, with the rise in cyberattacks and data incidents, organizations are finding that data minimization is actually a "must-have."

Historically, organizations have been weary of deleting data "just in case." That's why even now organizations struggle to determine what happens to projects, matters, files, and documents that have been completed or abandoned. A common practice among organizations is hanging on to them by putting them in a designated folder.

When unnecessary data and completed matters or projects remain in a workspace or virtual collaboration system, they create more risk. Just because a project or data is no longer viewed as "necessary" does not mean that its contents are not sensitive. These projects could contain client information, internal memos, trade secrets, financial records, and other information that – while no longer of use to your organization – is plenty relevant to malicious cybercriminals.

It is imperative to dispose of data through scheduled deletion. This ensures that unnecessary data isn't floating around longer than it needs to be, reducing the chance of exposure in a breach.

Not only that, if sensitive data such as client information were to be stolen, this leaves organizations on the hook for even further costs in regulatory penalties and reputational damage.

If your organization hasn't begun planning its data minimization journey, it's time to start now.

5 Archive Important Data

Deleting extraneous data can help alleviate data chaos and reduce cybersecurity risks. But what about the data that needs to be kept even after a project ends or a matter is resolved?

The most important data should be stored in an off-premises storage location such as Amazon Web Services (AWS) or Microsoft Azure.

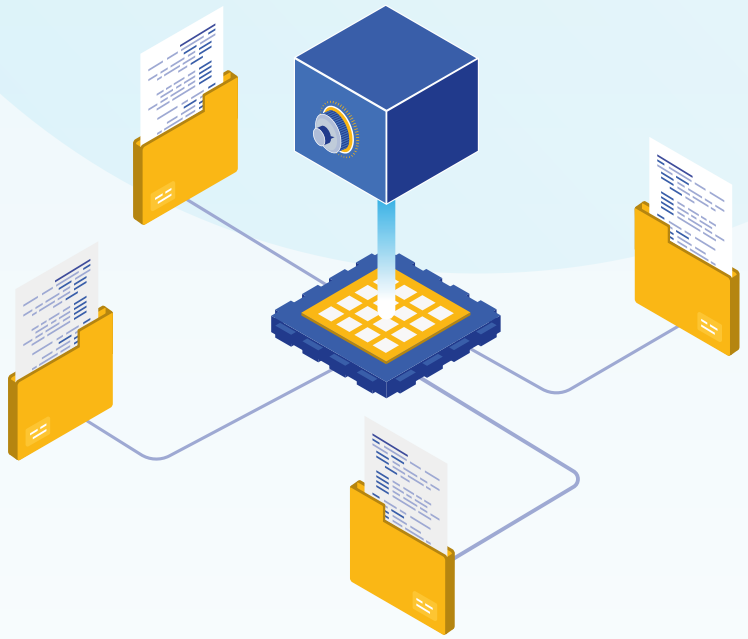
By storing documents in your organization's private AWS or Azure tenant with the metadata and security stored in software solutions, your organization has an archive that serves as a back-up in case of a breach or outage. Users can access the archive through a One-Time Password (OTP) and download or check-out documents through a profile search. Once systems are back online, service desk or end users can check the documents back in.

If a breach were to occur, your organization would have peace of mind knowing that hackers cannot hold data ransom over you because you have that document archived. Not only that, but your organization can still access this data and maintain business continuity.

For these data minimization elements to be effective, it's important to develop a data minimization strategy beforehand. One of the first steps is understanding each of your departments data needs. Since some departments require deletion of data after a few years while others might have a more detailed process of archival, determining these requirements is key to starting this process.

Data minimization policies remain ineffective if not implemented across collaboration systems. Applying such policies only to one system leaves the other systems unregulated. A practice that only intensifies your organization's challenges and vulnerability towards cyber-attacks. That's why all systems where data is stored and processed must be aligned with your organization's data minimization strategy.

To get the best results out of this step, it's important for it to be automized. A possibility that is currently offered only by third-party solutions.



6 Report on Inappropriate Activity

The best way to detect inappropriate activity is to monitor activity that appears abnormal, such as users deleting documents, moving files and folders, downloading too many files, accessing files irrelevant to their position, and more. These can all be signs that users are unaware of your organization's data protection policies, or worse, intentionally creating cybersecurity risks internally.

To remedy this, organizations should run frequent analytic reports to monitor user activity.

These reports can track if users are accessing too many documents, downloading exorbitant amounts of assets, or copying and deleting files when they shouldn't be. Information from these reports can help your organization prepare for internal threats, as well as the potential for internal errors that lead to outside threats.

7 Privileged Access Management

Most collaboration systems' Service Desks grant too broad of access out-of-the-box. Administrators are given far-reaching access and have permissions for far too much data.

If an administrator were to have their passwords or credentials compromised, the hacker or cybercriminal in question would have access to a wider array of files than the typical user.

Privileged Access Management (PAM) is a strategic approach to cybersecurity that centers around monitoring all users and their levels of access across a given workspace and giving users and administrators the least amount of access privileges necessary.

By reducing the number of files and data your admins have access to, the less risk there is of a data incident. Overall, a PAM strategy enables organizations to create a more user-friendly environment to record all IT & sensitive data related activities.

Bringing It All Together

Establishing this seven-step data protection plan will go a long way in helping your organization mitigate the risks leading to a "bad day." In the event of a breach, your most important data will have been properly secured and the excess data will have been deleted. This results in less risk and a lower chance that a hacker will be able to ransom any files.

As collaboration systems enable these processes to be performed only manually, it can be time consuming and requires a great deal of resources. On top of that, when provisioning is done manually it can lead to further human error resulting in more risk and vulnerabilities.

To avoid these challenges, organizations should turn to a software solution that can automate these processes and carry them the extra mile.

Prosperoware CAM is just that solution.

Prosperoware CAM is here to help

Prosperoware CAM is a Software-as-a-Service platform (SaaS) for adoption and governance of collaboration systems. It allows organizations to provision, classify, protect, move, and minimize data, mitigating data chaos and reducing risks related to privacy & cybersecurity.

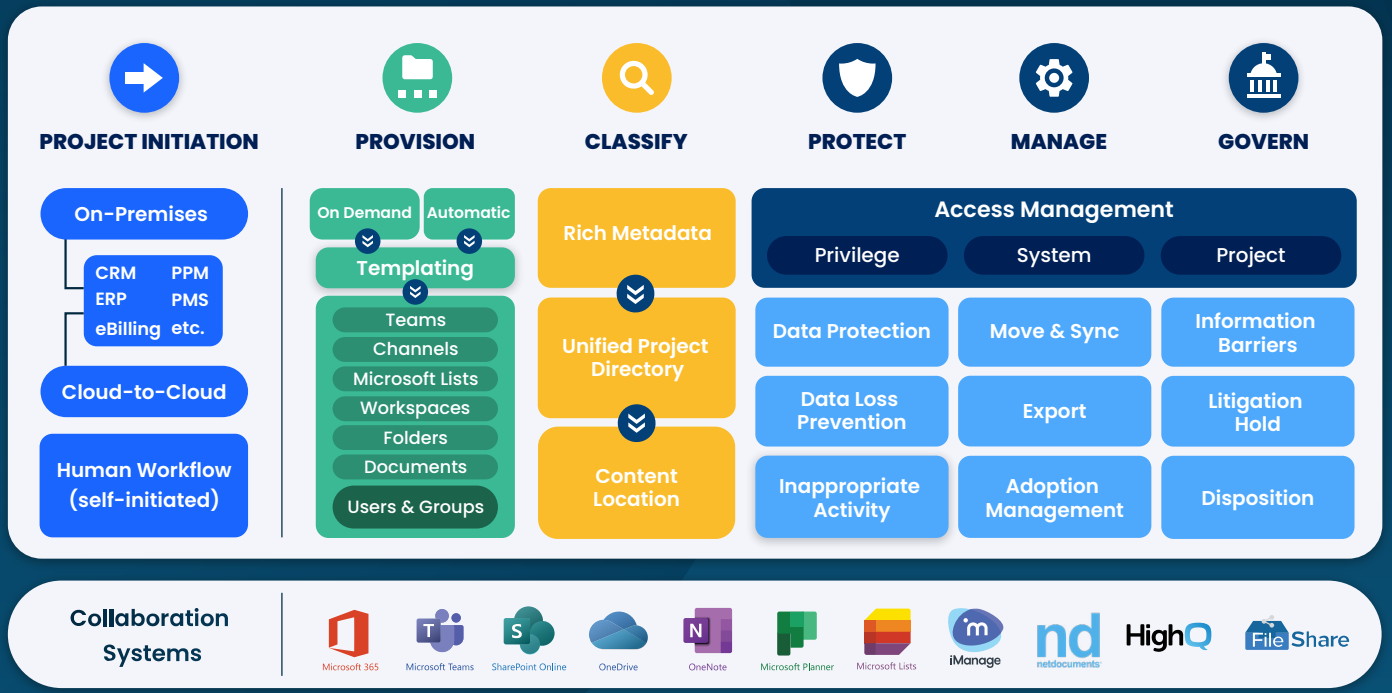
CAM integrates with Microsoft 365 (Microsoft Teams, SharePoint Online, OneDrive, OneNote, Planner, Lists), iManage, NetDocuments, file shares, HighQ, and more to come.

CAM enables organizations to implement process-driven collaboration by provisioning logical locations for users to place data and adding rich custom metadata to empower users to locate data and risk management teams to understand context so they can apply the right security and minimization policies.

CAM supports access and privileged access management through assigning role-based permissions to internal and external users with expiration dates. The platform's data protection capabilities ensure that organizations have an archive of their sensitive documents, ready to access them through a One-Time Password (OTP), in case of an incident.

CAM allows in-depth reporting and analytics through a SQL-based interface where technical and non-technical users can run any query they need and generate reports across collaboration systems. Finally, CAM's data minimization capabilities ensure that organizations can set trigger-based disposition policies with approval workflows or place content on litigation hold.

How does CAM work?



Key CAM features include:

- Provisioning of workspaces, Teams, channels, lists, users & groups, and folders from Project Portfolio Management, CRM etc., or through a human workflow using readily available templates
- Rich, custom metadata for project or document context
- Get a bird's-eye view of your projects through a Unified Project Directory
- Classify data through rich custom metadata enabling easy content location for end users and understanding of context for risk management professionals
- Protect data by managing internal & external users and groups across systems, assigning relevant roles and granting or restricting permissions. Integrate common ethical wall systems to improve governance. Set data protection policies by storing your documents in your own AWS or Azure cloud, while only storing document metadata and security to CAM – enabling you to conduct profile searches & download documents in case of an outage through a One-Time Password (OTP)
- Effectively move data within & between collaboration systems to strengthen governance & respond to client requests
- Minimize data you no longer need, mitigating security risks & reducing costs of storing unnecessary data. Set trigger-based disposition policies to ensure unnecessary documents are minimized

LITERA

prosperoware

We help teams collaborate more efficiently and securely

About Us

We are a thought-leading SaaS & enterprise software company for collaboration systems. Our core competency is our expert understanding of enterprise systems, data and processes in organizations, and developing technology for digital transformation. We develop software for improving adoption & governance for collaboration systems and financial matter management. Our customers include 50% of the Global Top 20 and AmLaw 200, 67% of AmLaw 100, 25% of UK Top 50, more than 40 global corporations including Fortune 500 and the Big Four accounting firms.

Contact Info

North American sales

+1.484.434.8200

EMEA and APAC sales

+44.203.880.1550

Support and development

+1.312.462.3800