White paper ERAM

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

INDEX

SUMMARY

Data management is becoming increasingly important to companies of all industries. Unstructured data – stored in the form of documents as compared to structured data stored in the form of easily queried databases – is the biggest challenge, comprising as much as 80% of an organization's file system.

Manually managing the file system is an incredibly complex undertaking. Organizing user access to data using standard Access Control List (ACL) settings and Active Directory (AD) information is a difficult process, with determining who actually has access to certain data and any associated changes or activity made extremely complicated. Analyses have demonstrated that the access rights within many file systems are polluted and access control is not properly organized.

ERAM is Tools4ever's data management solution, consisting of three key functions that help you significantly simplify and optimize the active management of your file system:

- Collection – This functionality provides system administrators with fast yet detailed insight into effective rights and usage per user and per file. ERAM correlates all of the file system's ACL settings and audit info with AD's information regarding users and groups – creating an up-to-date database with which to quickly and easily search for all user and file information. This database is required to support the second key function.

- Reporting & Analysis – ERAM's reports and analysis allows system administrators to utilize the information in this database to – among other things – clean up actions and detect pollution. Hereafter, the process and structure of ongoing data management can be optimized and future audits are easily conducted – establishing a solid basis for the third key function.

- Data Ownership and Self-Service – ERAM's data management controls facilitate assigning ownership of shares and directories with the proper "data owner" (e.g. manager, department head). By enforcing a uniform method, ERAM prevents the future creation of new pollution. Additionally, this key function supports self-service data management, where employees can request access from the rightful "data owner" online and approvals are then correctly processed across the organization's integrated systems.

ERAM is a complete solution for optimal file system management. No longer will you have to struggle with outdated and polluted access controls. Your IT department retains insight into the most current access rights and their use at any moment. More importantly, your "data owners" maintain responsibility for managing access to their resources – with request/approval processes realized as much as possible via self-service rather than by overburdening your IT department with tedious helpdesk tickets.

INTRODUCTION

Data management is an increasingly critical business process for virtually all organizations, not only for its crucial relationship to successful operations but also due to ever-more strict laws and regulations mandating that companies maintain a consistent grip on stored and utilized data. This is especially enforced in regards to data containing sensitive and Personally Identifiable Information (PII), with mistakes and errors resulting in severe financial and reputational impacts.

Emphasis has traditionally been placed on structured data – stored in databases, easily queried and used and edited in business applications – despite the maturity of business applications elevating access to a continually high standard and relegating its security to less of an active concern. The right expertise and approach easily achieves proper structured data management. Additionally, structured data only comprises roughly 20% of the file system, whereas the remaining 80% comprised of unstructured data often presents the real security challenges.

Unstructured data stored in the file system – such as documents, presentations, Excel files and videos that lack more rigid classification structures – can remain for decades without proper organization, management, or cleanup. Managing user access rights to the correct folders and files remains difficult for IT and helpdesk employees, as, in reality, they hold little insight into which specific users have access to which specific files. It is also difficult for new employees to determine the company data to which they have access. Instead of secure and proper management, access to unstructured data is often organized on an ad hoc basis.

The impact of this loose-at-best management is significant. Your company operates with greater risk of potentially misusing confidential data and, during audits, may be found non-compliant. Any efforts made to correctly managing personal data in business applications is immediately negated by Excel spreadsheets containing the same information in an unmanaged file location on your servers. Further, system administrators waste substantial time and value answering and solving access management issues – placing among the top three of frequent helpdesk calls for many organizations. Ultimately, your IT architecture as a whole will perform far more efficiently if pollution and unnecessary access rights are cleaned up.

Fortunately, there are a few answers to unstructured data problems. These files were traditionally stored in Document Management Systems (DMS). Online portals, such as Sharepoint Online, have seen recent increases in adoption to move access control to an organization's employees. However, it is often not possible to implement these migrations company-wide and the same file management issues remain. Tools4ever has addressed these management problems by developing Enterprise Resource Authorization Manager (ERAM) as the solution for all your unstructured data management needs.

With ERAM by Tools4ever, you can now manage the unstructured data in your file system without having to migrate anything or circumnavigate day-to-day operations as such substantial manual changes would normally require. Instead, ERAM allows the data to remain in the file system, where a system administrator can organize it during the course of an average day. ERAM provides easy insight into users' rights, reporting and monitoring to accurately track and analyze unstructured data and tools to organize Data Ownership according to business roles while empowering employees via Self-Service request/approval processes.
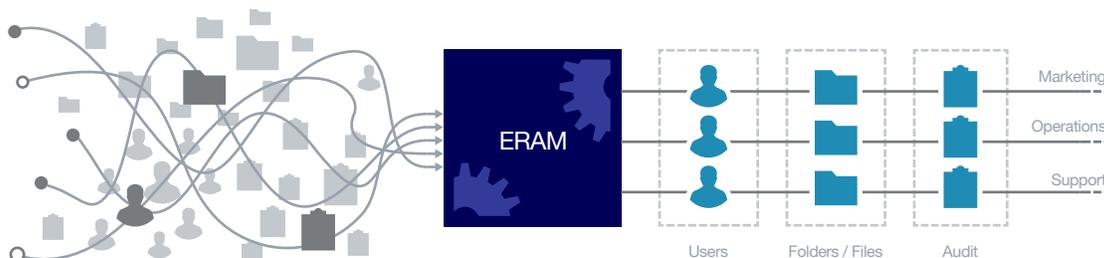
ENTERPRISE RESOURCE AUTHORIZATION MANAGER

Managing access to data in the file is a challenge without the right solution. Standard Microsoft tools - Active Directory Users & Computers (ADUC) for AD, and Windows Explorer for the file system – do not provide the ability to easily determine who has effective access. Further complicating this challenge is the fact that many file systems have been in place for over a decade while under the purview of multiple employees in that time. This is often due to events such as mergers and acquisitions, and, as a result, access rights are mostly (and seriously) contaminated.

Not only is it difficult to manage access on a contaminated file system, but it is also not possible to combine audit and access info for clear reporting and analysis. Without said information, it is impossible to properly organize the file system, or enforce established standards and procedures moving forward. Needless to say, there are numerous barriers in place preventing effective manual management efforts.

ERAM (Enterprise Resource Authorization Manager) offers a better alternative to existing, limited tools by ensuring pollution can be cleaned up for optimal file system management. ERAM consists of three key functions – summarized below and explained with greater detail on the following pages.

1. Collection provides system administrators with fast yet detailed insight into effective rights and usage per user and per file. ERAM correlates all of the file system's ACL settings and audit info with AD's information regarding users and groups – creating an accurate and current database with which to quickly and easily search for all user and file information. Collection can be executed on an ad hoc, periodic basis or scheduled to run automatically to ensure the gathered information is up-to-date.

2. The Reporting and Analysis functions compile comprehensive reports and analytics driven by ERAM's Collection-built information database. System administrators can improve and optimize data management by – among other things – detecting pollution and performing the appropriate cleanup actions. With Reports and Analysis, it is possible to determine and revoke existing employee access that has gone unused and deemed unnecessary or noncompliant. This function also facilitates auditing the use of data.

3. "Data Ownership" and Self-Service consist of the ongoing and active management tools for capitalizing on the strong starting point provided by the analysis of data usage within the organization. This function allows you to utilize the collected information about which shares and folders are used by which users and groups to reorganize and appoint their management to the best owner in the organization, e.g. managers, department secretaries, project managers. ERAM provides accessible and user-friendly tools to perform these sophisticated activities so that employees and "Data Owners" can independently operate according to the established procedures and without helpdesk intervention.
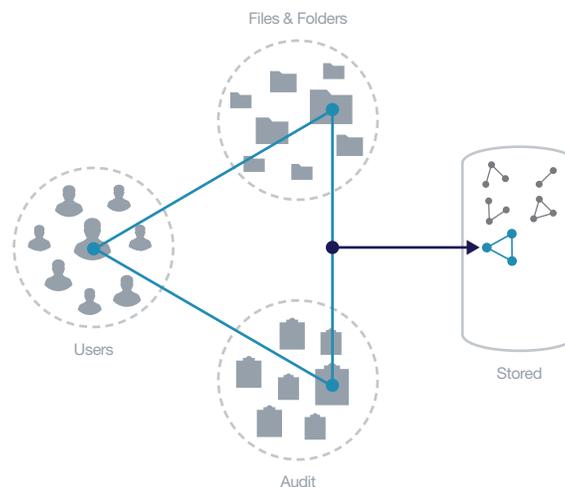
COLLECTION

The Collection functionality forms the basis of ERAM to help answer questions such as the following:

1. Who has access to which folders?
2. Where does "Employee X" have access to?
3. Who owns a folder?
4. What/where exactly is the dangerous pollution in the file system?

Without additional tools, these types of questions can only be answered if a system administrator combines information from different source systems. Only by combining ACLs and audit information from the NTFS file system with AD information about users and groups is a system administrator able to find the answers – an extremely laborious and time-consuming process.

By comparison to these painful methods, ERAM ensures that file system data and the answers to the preceding page's questions are readily available and accurate. ERAM accomplishes this via its database that correlates current ACLs and audited NTFS data with up-to-date information regarding AD-managed users and groups. This database provides an immediately-processed overview of users and resources at any given time to quickly answer the previous or related data management questions. Additionally, all user activity conducted upon files and folders is logged and processed within the database to provide usage insight over a given period of time.

ERAM Collection functionality: The ACL file, AD users and group and NTFS audit information is continuously collected and correlated in a SQL database.

ERAM COLLECTION, BASE FOR ADDITIONAL APPLICATIONS

With ERAM Collection functionality, system administrators retain a powerful source to provide detailed answers to questions regarding user rights, access to files and the use of those files.

ERAM Collection, therefore, forms the foundation for its additional functions. By using the information stored in the SQL database as a source, it is possible to easily provide comprehensive reporting, monitoring and audit functionality as well as effectively manage data ownership in the organization. These functions will be discussed with greater detail in the following sections.

REPORTS AND ANALYSIS

The ERAM collection functionality allows system administrators to instantly check the access rights of a specific user. Alternatively, they can check who has access to a specific file or folder and whether that access is actually used (auditing).

REPORTS

By default, ERAM has an extensive set of report templates regarding the status of the file system's security settings. These reports are based on SQL queries. Because the ERAM database model is fully open and documented, you can also use all common reporting solutions.
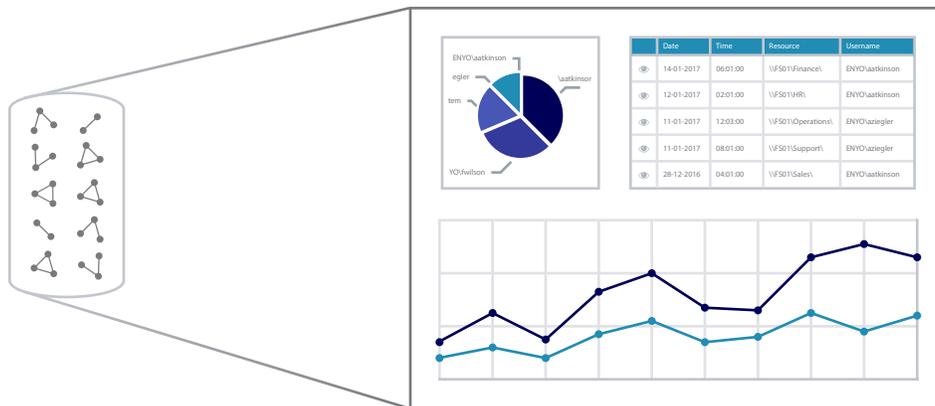
In addition to the collection functionality, ERAM has extensive reporting and analysis features.
This allows the file usage to be analyzed and optimized quickly and effectively.

With ERAM's reports, it is possible to detect and clean up pollution based upon the gathered information. For example, it is possible to see which employees retain access to a folder without ever utilizing it. A similar but reverse report would provide insight into which sensitive information has been made available to employees or user groups who do not or should not have access. The various access rights can be cleaned or modified based upon ERAM's analysis.
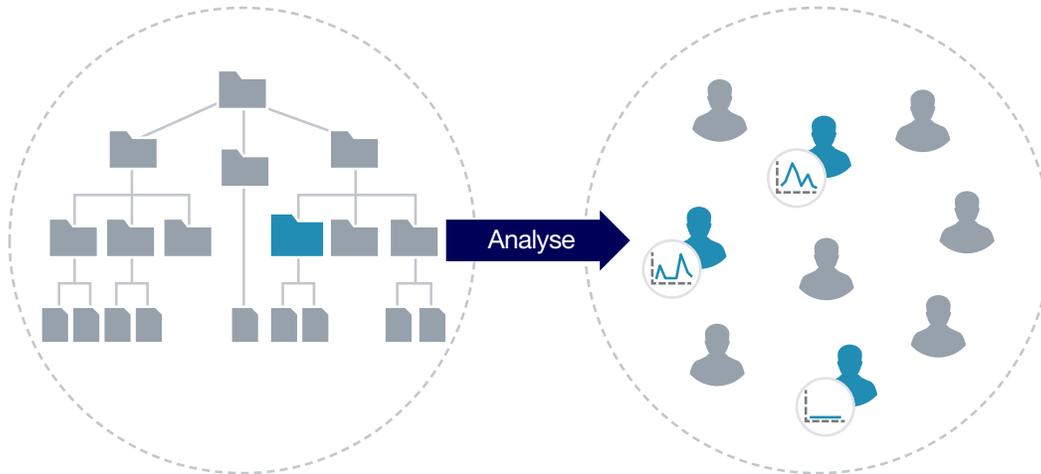

ERAM supports the system administrator in the comprehensive analysis of data usage. For example, which users make intensive use of certain data? Which users don't?

ERAM always provides up-to-date information about file access and file system activity to clean up your data management - keeping your data not only manageable but also preventing its potential leakage.

ANALYSIS

Has your organization ever experienced a data leak? Or do you have another reason to analyze access to certain files, folders or shares over a longer period? For these reasons, ERAM offers audit trail features. Extensive analysis is easily conducted using all of the longer-term information regarding access rights, changes to those rights and the current usage of files that has been collected and stored by ERAM. Who has access to certain files over the past few months? What actions took place? From which IP address? ERAM quickly and easily answers these and other, related questions.

1340 AD Users | 350 AD Groups

1,800,000 files | 300 shares | 24 Tb
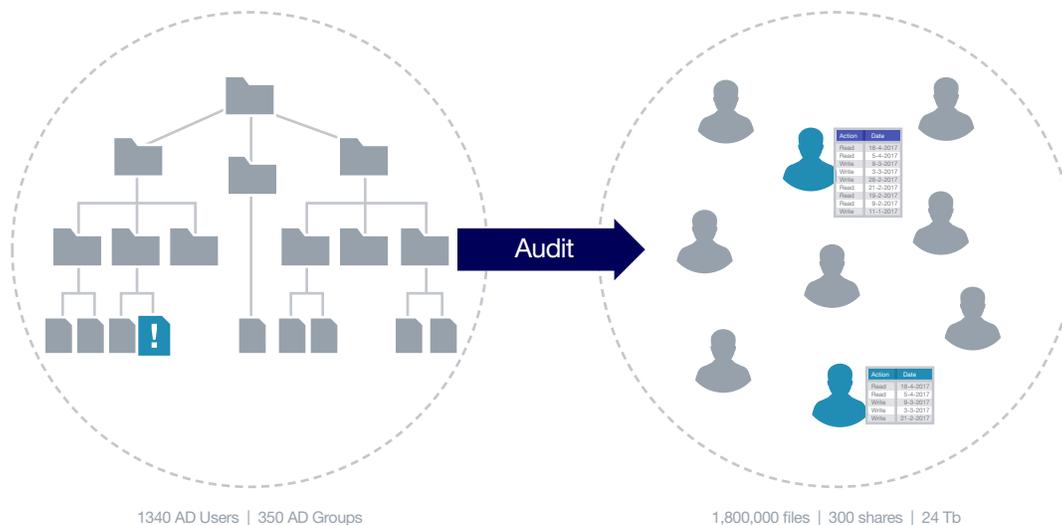
Using the audit trail feature, ERAM can provide effective and quick insight regarding access to and the use of files and folders.

Employees require access to an organization's data and who should have access to certain information is best determined by those employees. Department managers, self-lead teams, team leaders, project managers, secretaries and more have the most insight into the realistic usage of data within day-to-day operations. Determining and managing actual ownership of the data should fall under the responsibility of the organization's hierarchy rather than be simply bolted onto the IT helpdesk's purview. That stated, how do you determine which employees best fulfill these ownership roles and what data they are responsible for?

ERAM helps answer these questions by providing reports that identify both potential data owners within the organization and the data they are responsible for. Further, ERAM offers the data owner the ability to manage access independently. This topic will be expanded upon in the next section. Ownership of the data

DATA OWNERSHIP MANAGEMENT AND SELF-SERVICE

ERAM makes it possible to map and clean the structure of and pollution within the file system. Building upon this, it is critical that the organization prevents future pollution and that ongoing management is handled as efficiently as possible. ERAM's Data Ownership and Self-Service functions meet this need for active and proper management.

CAUSES OF POLLUTION IN THE FILE SYSTEM

Pollution in the file system often has two main causes:

1.   The ownership of the data is not regulated. Often within organizations, the clear owner of a specific file share or particular folders is not the same person responsible for managing it. IT is typically burdened with this task and official requests for access rights are directed to the helpdesk. This leads to the day-to-day management of actions and changes being conducted without an understanding or reference as to their relationship with the business-usage of the data.

2.   The organization of the management procedures is not in order. Over time, organizations face all kinds of changes: changing administrators at the IT help desk; changing management procedures; changing management insights; and mergers, reorganizations and incomplete migrations are only a handful of examples. These changes make it extremely difficult to manage the file system according to consistent procedures and specifications, leading to ad hoc efforts - the perfect recipe for further polluting the file system.

ERAM not only addresses the cause of both scenarios, but as the following pages will demonstrate, it supports the future management of the system.

The first step of "Data Ownership" is to appoint a data owner for every part of the file system (shares/folders) to be responsible for its day-to-day management. It is crucial that this individual is familiar with the data and how it relates to the business' operations, as this knowledge helps them determine which other employees require access to that data.

ERAM facilitates this ideal data ownership structure. The solution provides reports that make it far easier to understand which data is used, by what groups and which user should logically be appointed its owner. ERAM provides each data owner with the means to perform daily management. They may easily create new folders (ERAM transparently creates the corresponding user groups), invite users for those groups and determine the available access rights, i.e. read, read/write, full, per group regarding the files, folders or shares.

ERAM provides up-to-date overviews and insight of the existing data shares and their respective owners, ensuring that corresponding data ownership is immediately adjusted or maintained in response to changes and extensions of the share structure. ERAM also accounts for scenarios such as a data owner leaving the organization, actively tracking activity to determine and appoint new ownership.

1340 AD Users | 350 AD Groups

1,800,000 files | 300 shares | 24 Tb
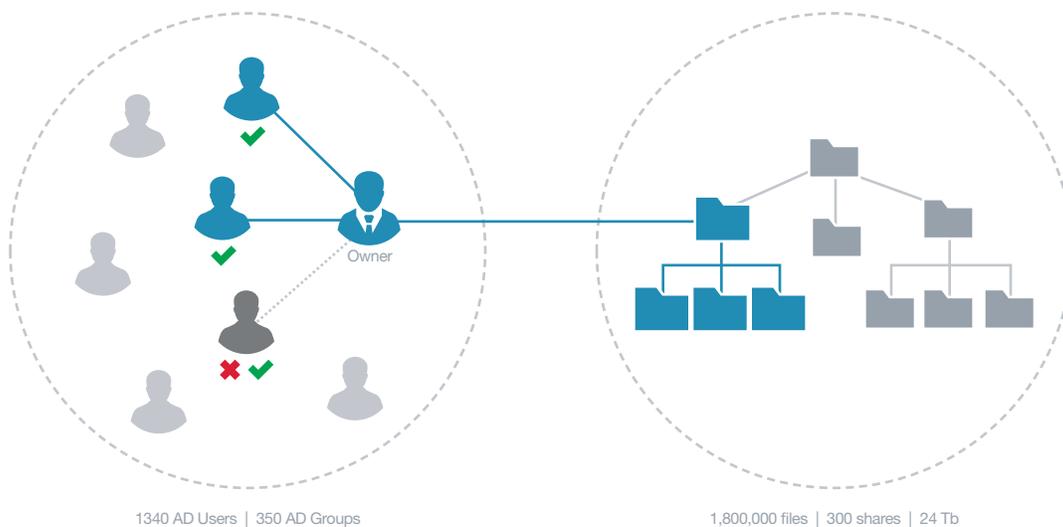
ERAM takes care of the data ownership management within the organization. The appointed data owners can independently manage their own data storage.

ORGANIZATION OF MANAGEMENT PROCEDURES

As previously stated, direct access to AD and ACLs on the file system provide too much freedom for data owners. With this lack of restriction, they are given the risk- and pollution-causing ability to organize user rights at an individual level rather than via group structure. The consequences of such poor management may include – among others – intertwined rights on deeper levels of the file system or group names that do not match the folder name / path and deny / block inheritances.

ERAM removes the capability to mismanage access rights by enforcing unambiguous and structured user management. ERAM's combination of clean-up exercises and user management decontaminates the file system and prevents re-pollution.

ACCESS TO FOLDERS VIA SELF-SERVICE FOR END USERS

ERAM gives data owners the ability to efficiently manage their own data shares on a daily basis, with the next step being the transition to self-service access request/approval processes for end users. Via the self-service portal, individual employees have an overview of all possible folders and shares to which they have access or may request access. Employees can terminate unused or unwarranted access themselves as well as submit new requests for direct access. In the latter case, ERAM sends a request to the data owner of the relevant folder, who then decides whether access is granted. Once approved, ERAM ensures that the applicant actually receives access to the relevant data. The data owner always has an up-to-date overview of all employees who have access and can add or remove users as necessary.
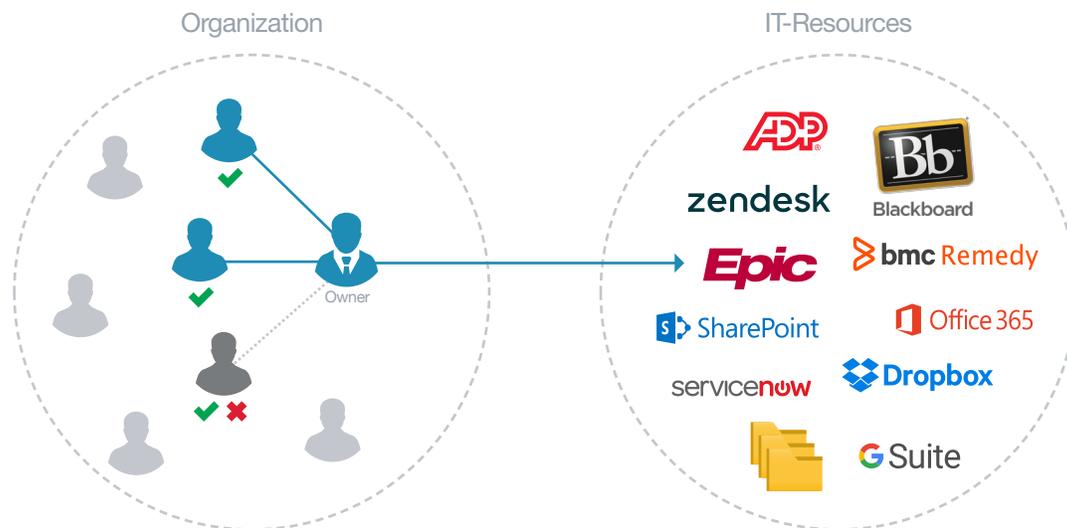
Data self-service. In addition to application management via the self-service portal, users can now also request online access to specific data files, folders or files.

AUDITING OF USER MANAGEMENT

We previously described the audit functionality of ERAM with respect to file and folder changes. If necessary, the audit functions make it possible to reconstruct who has access to certain data in the file system and which user has made which changes at which time – completely reconstructing the "timeline" of files.

However, ERAM provides greater audit capabilities. Once ERAM facilitates transferring the data ownership from IT to the correct owners in different departments and according to business roles, reconstructing their organizing activities becomes an integral part of overall management. ERAM's audit function addresses this as well.

ERAM records all of the changes to user rights performed by a data owner or one of their "delegates." These audit records allow security officers to report when and by whom certain data was accessed as well as which employee granted the specific access.

TOOLS4EVER

ABOUT TOOLS4EVER

Tools4ever is one of the largest vendors in Identity Governance & Administration with more than 5 million managed user accounts. Since 1999 Tools4ever has developed and delivered several software solutions and consulting services, such as Identity & Access Manager (IAM) and HelloID (IDaaS).

Tools4ever has many integrations and strategic partnerships with software vendors. This software is used by these vendors and vice versa. For example, Tools4ever works with software from TOPdesk and TOPdesk works with our software.

Tools4ever's Identity Governance & Administration solutions are installed in organizations from various sectors ranging in size from 300 to over 200,000 user accounts.

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

TOOLS4EVER NEW YORK

300 Merrick Road, Suite 310	General	+1 866 482 4414	Information	nainfo@tools4ever.com
Lynbrook NY 11563	Support	+1 516 482 7525	Sales	nasales@tools4ever.com
USA	FAX	+1 516 825 3018	Support	support@tools4ever.com

TOOLS4EVER WASHINGTON

11515 Canyon Road E	General	+1 888 770 4242	Information	nwsales@tools4ever.com
Puyallup WA 98373	Support	+1 253 770 4823	Sales	nwsales@tools4ever.com
USA	FAX	+1 253 435 4966	Support	nwsupport@tools4ever.com