Omada

DO MORE WITH IDENTITY

HOW TO OPTIMIZE AND AUTOMATE IDENTITY MANAGEMENT PROCESSES TO ENABLE ACCESS GOVERNANCE AND CONTROL COMPLIANCE

Enterprises within the manufacturing industry typically operate in a market with thin margins and global competition. To sustain efficiency and cut down user administration cost while ensuring compliance with legislative and industry specific regulations are challenging concerns in manufacturing industries. Customers, partners, suppliers, and employees around the globe require system access, efficient automated processes, and management. To stay ahead in the global competitive market, manufacturing enterprises need to be agile and flexible while maintaining a high security level and clear business overview.

www.omada.net
info@omada.net

CONTENT

> Managing the difficult tradeoff between agility, security, and compliance is a significant challenge for manufacturers

1. Introduction

To remain competitive, manufacturing companies must be as agile as possible while managing complex ecosystems with suppliers and distribution channels, complying to regulations, and implementing new and innovative systems that support their business processes to provide efficiency increases through IT service automation.

Managing the difficult tradeoff between agility, security, and compliance is a significant challenge as manufacturers are often geographically dispersed, have a wide variety of on-premises and cloud-based systems, and need to work to tight margins to compete in price-sensitive business environments.

Many of the challenges within these areas can be addressed using an identity management and access governance solution that not only ensures the enforcement of security and compliance but also acts as a business enabler.

This e-book is aimed at IT / identity management professionals and provides an overview of some of the critical challenges manufacturing companies face that can be addressed using a next generation IAM solution with identity governance capabilities. It also gives guidance on the identity management and access governance functionality that should be considered to help make business processes more efficient for the specific challenges of a manufacturing environment.

2. Challenges Facing the Manufacturing Industry

Manufacturing companies must navigate many challenges to remain competitive in the fierce markets in which they operate. They need to manage the complexity of the supply chains, adhere to strict regulations, continue to innovate their business systems to remain agile, and efficiently integrate partners, employees, and contractors into their systems.

This section outlines these areas by explaining the main challenges that manufacturing companies need to overcome. Once these challenges are understood, the opportunities to address them using identity management and access governance solutions are discussed.

Complex Ecosystems

Manufacturers need to share internal information and engage with business partners, vendors and distribution channels but need to protect their intellectual property by controlling levels of access.

Regulatory requirements

Manufacturers need to comply with a wide variety of industry specfic regulations and legislation such as GDPR and SOX. Policies must be managed across complex platforms using identity management and access governance.

Cloud Migration

Increasingly, manufacturers are moving applications to the cloud to become more agile and efficient, However, migration is not always an option for legacy applications which leaves them with the challenge of managing both on-premises and cloud-based applications.

Securing Complex Ecosystems

Manufacturing companies need to participate in highly complex ecosystems to be competitive. Whether they are working with business partners who supply them with raw materials, works-in-progress or specialist parts on the production side, or they are using companies in their distribution channel on the sell side, manufacturers need to manage a series of complex relationships with multiple parties.

The increasing complexity of partnerships, the move towards globalization, and the reduction in time-to-market commitments mean that manufacturing organizations are required to share more information with partners to remain competitive.

To ensure their ecosystems deliver maximum value for them, manufacturers must ensure all parts of the supply chain are working together towards common goals. To achieve this efficiently, manufacturers are increasing the digitization of their supply chain to enable them to share the latest information about product designs, parts requirements, customer order forecasts, marketing activities and much more.

Control the distribution of sensitive information

While it is essential to be as open as possible with collaboration partners, it is just as critical for manufacturers to control the distribution of sensitive information. Intellectual property is how manufacturing companies derive their revenue and can account for more than 80% of a company's value. For example, if the login details of a design engineer were to be compromised, complete sets of design drawings could be stolen and used to create accurate imitations that would significantly reduce the value of the 'original product' in the open market and hence the company itself. With more sharing comes more risk of compromise to intellectual property if access is not strictly controlled on an ongoing basis.

Manufacturers can set up direct access into their network using virtual private network (VPN) technology to share information held in in-house applications. While this solution achieves the goal of providing partners with the access they need, it requires time-consuming management, needs additional networking hardware, and is difficult to govern. Human error or oversight could lead to granting the wrong access to partners or access enabling access long after it is needed. This could lead to leaking of confidential data.

Migration to the cloud and adoption of directory services such as Microsoft Azure Active Directory improves the management aspects but still requires companies to ensure that they provide adequate security and governance to protect intellectual property. Many companies are not giving adequate attention to setting up security on cloud platforms leading to the risk of data breaches. They also need to provide collaboration partners with access to business systems in a timely fashion, by enabling automation of access management.

Regulatory Requirements

Manufacturing companies must comply with many regulatory requirements. While some depend on the type of manufacturing, others are more widely applicable. An Identity Management and Access Governance solution can help manage a wide variety of legislation requirements.

Sarbanes-Oxley Act (SOX)

Publicly listed manufacturing companies are required by law to comply with the Sarbanes-Oxley Act (SOX). While privately held manufacturers are not required to comply, many still adopt some SOX provisions as they make good business sense even though they will not face serious penalties for not observing all aspects of the act.

SOX involves ensuring good corporate governance and financial disclosure. As IT business systems are used to store and analyze financial information as well as generate reports demonstrating compliance, it is important that internal controls are in place to ensure they are secure and locked down against any potentially fraudulent activity.

Public manufacturing companies face significant penalties if they do not comply with SOX. These penalties include substantial fines and, in extreme cases, prison sentences for their executives. While an identity management and access governance solution alone does not make a company fully SOX compliant, the reduction in fraud, policy management, and compliance auditing play an important part in helping support a company's compliance initiatives by providing the capability to demonstrate consistent enforcement of internal controls.

General Data Protection Regulation (GDPR)

Any organization that collects, processes and stores privacy data of European Union citizens needs to be compliant with the General Data Protection Regulation (GDPR) regardless of where they are based. Failure to be compliant could result in a fine of 4% of their global turnover or €20 million, risk of reputational damage, and exposure to lawsuits.

GDPR sets out a series of data protection principles that need to be followed to be compliant. This process starts with understanding how personal data is collected, processed and stored. After an understanding of what the data is and where it is stored, organizations need to ensure that they take "appropriate technical and organizational measures" to protect it. Also, they must report any data breaches to both the authorities and those affected within a given timeframe within 72 hours.

Identity management and access governance solutions help organizations become GDPR compliant by giving them visibility and control over who has access to specific systems and data as well as enabling them to demonstrate who approved each level of access over time.

Annual Study of Intangible Asset Market Value from Ocean Tomo, LLC

http://www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study/

Migration to the Cloud

Up until recently, manufacturing companies have been reluctant to move their business-critical applications to the cloud. They have held back for a variety of reasons including security fears, concerns about network latency issues affecting their time-sensitive applications, and the reliance on legacy systems.

Manufacturing companies now realize that relying on lean-manufacturing methods alone is no longer enough as all their competitors are implementing the same techniques. To differentiate themselves, they need to look at ways to adapt to new market conditions where customer requirements are changing faster than ever before.

This realization has accelerated a significant shift with many organizations either addressing the concerns or realizing that the considerable benefits of adopting a cloud-first strategy far outweigh the risks. A recent survey at the Salesforce Manufacturing Summit in May 2017 found that only 25% of respondents were using enterprise cloud apps but this was expected to rise to 70% by the end of the year.

Manufacturing companies cite many reasons for moving their applications to the cloud including operational efficiency, application and partner integration, management and analytics of data and enhanced security. More generally, the move to the cloud can be summed up by the increase in efficiency and those that do “exhibit higher average labor productivity compared to manufacturing firms that are not cloud adaptive”.

Common applications suitable for cloud migration include:

- Enterprise Resource Planning (ERP) – to enable sharing of production information across internal departments and with external business partners
- Product Lifecycle Management (PLM) – requires extensive data management across different organizational boundaries both within the company and potentially with external business partners
- Configure Price Quote (CPQ) – requires consolidation of data from a variety of systems across the company including cost-of-goods, local factors such as currency conversions, competitive pressures, product availability, and delivery times
- Financial applications – requiring input from different divisions in different geographies which will then be used to produce reports across the company to facilitate decision making
- Digital manufacturing systems – facilitate the communication between globally distributed teams which means the designers do not have to be located close to the manufacturing plant

---

U.S. Department Of State – Directorate of Defense Trade Controls -https://www.pmddtc.state.gov/index.html
Manufacturers Must Move to the Cloud to Stay Competitive
http://www.industryweek.com/sponsored/manufacturers-must-move-cloud-stay-competitive

”How Cloud Computing Enables Modern Manufacturing” - American Enterprise Institute – June 2017

While they see significant efficiency gains in moving to the cloud, many manufacturers are still reluctant as they see the migration as adding another layer of complexity or risk to the challenges they already face. For example, some believe that sharing product design files from Computer Aided Design and Computer Aided Manufacturing (CAD/CAM) systems is too risky as they contain confidential intellectual property and future product designs. In other cases, it may not be possible for companies to migrate large, highly complex, highly integrated, legacy plant-floor systems to the cloud quickly and efficiently due to their original design.

So, as manufacturing companies do not want IT to be on their critical path to growth, they usually find themselves adopting a cloud-first approach deploying new applications in the cloud where possible while maintaining on-premises applications for legacy systems. They will migrate existing business systems over to the cloud if a valid business reason can be identified.

If identity management and access governance in these hybrid environments is not managed correctly, organizations expose themselves to significant security and compliance risks. However, if appropriate policies, procedures, safeguards and associated technologies are implemented then substantial efficiency gains can be realized while ensuring an increased level of security and compliance across the organization.

3. Threats to Manufacturers

Managing user access across the hybrid environment that manufacturing companies need to support can be challenging, time-consuming and prone to human error. Without the proper technologies, processes, and procedures in place, companies expose themselves to security and compliance breaches which could have a significant effect on their business operations.

These breaches could result in:

- Intellectual property being stolen due to compromised accounts
- Fines for non-compliance with data protection regulatory requirements
- Continued access to critical resources by former employees, contractors or business partners
- Employees with greater access rights than necessary to do their jobs
- Separation of duties violations due to lack of visibility into access rights across multiple systems
- Compromised privileged accounts resulting in significant access to unauthorized information

Companies need to do everything they can to ensure that the risks are mitigated as much as possible while still going ahead with new projects to make themselves more innovative and agile against their competition.

In the rest of this Special Report, Identity Management and Access Governance will be discussed regarding how it can help manufacturing companies improve their security, compliance, and efficiency as they manage their hybrid on-premises and cloud-based environments.

4. Identity Management and Access Governance in Manufacturing Environments

The threats faced by manufacturing companies need a comprehensive security plan that includes Identity Management and Access Governance as a central component. Identity Management Professionals have a pivotal role to play in making their companies more secure, compliant and efficient. By deploying the right elements in the right way, they can help significantly reduce the risks that their company faces due to these challenges.

Regarding the design and production side of manufacturing, they need to provide tools that control who has access to proprietary and confidential company information. This requires a solution that is not only sufficiently configurable to define sophisticated rules and policies but also systematically enforces them as it is extended to implement access requests and delegated access approvals to trusted third parties.

To support the sales and distribution divisions of their company, IAM professionals need to have granular and flexible control over how much of each application they grant access to for individuals. Employees and partners need to be given just the right levels of access to do their jobs. This access should be deprovisioned as soon as it is no longer needed to prevent risk associated with identity and data breaches. When manufacturers can quickly and confidently grant and deprovision access it results in the organization being more agile and efficient due to the sharing of appropriate information without increasing the risk to the business.

Orphan accounts – User accounts that do not have current employees or contractors associated with them. An orphan account usually occurs because of a legitimate user account not being disabled or deleted after an employee or contractor leaves the company. If these accounts are compromised, their use could go undetected for a significant period of time as they look like legitimate users.

Technical account – An account that is used by one system to access another. These accounts are generally not associated with an individual but could have significant access rights assigned to them which makes them a valuable target for an attacker.

Privileged account – An account, such as an administrator, that has elevated access to business systems. These accounts should have greater protection than standard accounts as they are more valuable to an attacker if breached due to their greater access rights.

Manufacturing companies are faced with a variety of challenges which involve keeping ahead of the competition, remaining within the law, and deploying increasingly advanced business systems to support their growth. Dealing with these challenges requires companies to continue to implement good governance which has complexities that manufacturers will need to address.

The following sections break down the different areas that need to be considered when implementing an identity management and access governance solution in a manufacturing environment.

Identity Management and Access Governance for Manufacturers

Identity Lifecycle Management
Automates the processes for creating, modifying, and removing users and access rights to ensure ongoing security and compliance.

Entitlements Management
A “single source of truth”for identities that defines and maintains what users are entitled to access.

Fulfillment and Connectors
Enables creating, updating or deleting user accounts in business system using connectors between the IGA and business systems

Access Request
Provides uses with a quick and simple portal to request, modify, or delete access to business systems.

Access Certification
Allows managers and system owners to grant or refuse access when they have made a request.

Workflow
A set of processes that automates business requests such as employees joining, moving or leaving to the right people for approval.

Policy and Role Management
Policies and roles ensure that actions taken within the IGA system follow internal and external guidelines and regulations.

Segregation of Duties
Controls to minimize policy violations or fraudulent activity by preventing toxic combinations of access rights based on business policies.

Reporting and Analytics
Generates audit trail reports to show who had access to which resources at points in time.

Identity Lifecycle Management

Identity Lifecycle Management (ILM) involves the creation and modification of user identities as well as the provisioning and deprovisioning of user access to business systems. These processes should be automated where possible to increase the efficiency of the IT department and to decrease the risk of human error which could introduce security and compliance risks.

Automated Identity Lifecycle Management (ILM) processes enable the granting of access rights according to defined roles, rules, and policies. This includes standard on-boarding and off-boarding processes of employees and contractors, as well as the granting or revocation of access to resources as a user's relationship in the organization changes.

Processes for core identity lifecycle management, role based access management, and segregation of duty, with integration to complex platforms such as SAP and Microsoft, support operational efficiency and security and is a contributing factor in retaining a competitive edge in highly competitive markets.

ILM helps manufacturing companies:

- ✓ Onboard employees and contractors with day-one access to the systems they need to do their job
- ✓ Create identities and manage access to their business systems for members of their complex ecosystems
- ✓ Ensure that ecosystem members are not granted greater access than is needed to do their jobs and do not retain access when it is no longer required
- ✓ Verify who has access to financial data, personal records, or defense project data to help them remain compliant with regulations such as SOX, GDPR, and ITAR
- ✓ Control identities and access to on-premises and cloud-based business applications to mitigate the risks associated with the adoption of a cloud-first strategy

Recommendation:
Manufacturing companies should ensure that the ILM solution can differentiate between different user community types such as contractor, employee, and business partner so that they can be managed differently as required. Due to requirements of manufacturing requiring flexibility, any ILM solution deployed should make it easy to move users between different communities without losing the history of their identity. This is necessary to accommodate changes such as contractors becoming full-time employees as well as partners moving employees between projects.

Control user access to business systems

Having ILM in place allows administrators to keep in control of the user identities and their access to business systems. However, due to the fluid nature of manufacturing workforces, the use of contractors to fulfill short-term projects, and the interaction between manufacturing companies and external business partners, it is necessary to verify the validity of existing Active Directory user accounts before implementing a system that manages the identity lifecycle of user accounts. This check includes confirming that there are no orphan accounts and that all technical accounts have an actual person owning them. This gives the business a known-good user account base to start from.

To do this, an Identity Management and Access Governance solution takes data from sources that contain the most accurate and up-to-date records of employees and contractors. This is referred to as an "authoritative source" and is often the company human resources system. This data is compared with actual Active Directory accounts that have access to business-critical systems. Accounts that cannot be matched to current employees or contractors will be flagged as orphan accounts for review. Similarly, technical accounts will be flagged as requiring an "owner" so they can be governed on an ongoing basis.

Once orphan accounts have been addressed either by matching them to an individual or by disabling them, the ILM update process will use changes in the human resources system to trigger processes to provision, change or de-provision user access rights. For example, if a new employee is entered into the human resources system, a workflow process will be started, and appropriate access granted to business systems based on their role, job title or profile.

In a manufacturing environment, the accounts created will be in the Enterprise Applications as all employees will have at least basic access rights to systems such as shared drives and email. Depending on their job role, they may be granted additional access to other applications such as ERP on a permanent or temporary basis.

Recommendation:
When considering functionality, three things need to be taken into consideration to ensure integration with applications:

- Application connectors – for linking to individual commercial applications
- Generic connectors - using standard formats such as flat files, database connectors (e.g. JDBC and ODBC), LDAP connectors, and web services connectors (e.g. SOAP and REST)
- Custom connectors – Software Development Kit (SDK) to create links to bespoke, in-house systems or systems not specifically supported by vendor or generic standards

The creation of custom connectors is particularly important in manufacturing where the access control to bespoke or legacy applications needs to be managed.

Entitlements Management

An important part of any Identity Management and Access Governance solution is the capturing, viewing, organizing and assignment of entitlements to an identity. The data describing identities, applications, accounts, entitlements, and controls are consolidated from different business systems within the organization. This collection of data forms the “single source of truth” of identities and what they are entitled to access and should include both on-premises and cloud-based systems.

As employees typically have several accounts spanning many different systems, it is necessary to match their accounts and associated entitlements so that a single identity can be created. This can either be done manually by the administrator or automatically based on matching rules. User account correlation is necessary to identify not only orphan accounts but is particularly important when enforcing separation of duties across multiple business systems.

As entitlements are identified, it is common to discover that many assignments use system naming conventions such as Active Directory security group names. These system names are usually obscure and not easily understood by end users. To make cryptic resource names understandable by non-technical users, they should be enriched with metadata using language that the business understands. Account, entitlement and control data is typically imported into the entitlement catalog in two ways:

- Flat files (e.g. CSV) exported from systems distributed across different parts of the company
- By directly connecting to applications

To directly connect to applications, connectors that can read from the target applications are required (see Fulfillment and Connectors section).

Fulfillment and Connectors

The processes of creating, updating and deleting of accounts in the business systems as part of the Identity Lifecycle Management process is referred to as fulfillment. To carry out these changes, Identity Management and Access Governance solutions use robust, non-intrusive connectors to link to the business systems.

The fulfillment process manages:

- The creation of accounts
- Requirements needed for accounts to be created
- Naming conventions

As well as account creation, fulfillment details how accounts should be managed when people leave the company – i.e. should their account be deleted, disabled or suspended. Best practices typically indicate that accounts should be disabled for a given period before being deleted. This allows the business to retrieve information if required after the person has left the company.

In addition to being able to connect with business applications to create and manage user accounts, connectivity to the company human resources system or systems is also important. As described in the section “Identity Lifecycle Management” above, the company human resources system is usually the most accurate list of current employees and any changes in their status which triggers changes to access rights in the business systems.

Access Request

To support end users as effectively as possible, there should be a quick and simple way for them to request, modify or delete access to a resource such as a shared drive or business application. Many solutions use the concept of self-service tools that look like shopping carts which users are used to seeing on online retail sites. To assist with the process, some of the portals make suggestions based on the user’s role or peer group access rights.

Ideally, in addition to supporting direct requests from end users, a self-service portal should make it possible for another employee such as a manager, personal assistant, or help desk support engineer to make a request on behalf of another user. To avoid presenting end users with technical jargon that is only understood by the administrators to describe resources, the self-service tools should be configurable so that plain English descriptions are displayed.

In addition to supporting employees, it should be possible for business partners who are granted access to systems to manage their users. This reduces the administrative burden on the IT department while ensuring that business partners get the access they need.

Access Certification

When a user requests access to a system, typically through a self-service portal, the system owner or a designated manager can determine whether to grant or refuse the access.

The reviewer should be presented with all current entitlements and roles associated with the specified user. This gives them a complete overview of what the user already has access to which will help them determine whether the additional access should be granted. The reviewer will be able to schedule the frequency at which certifications are run so that the access rights granted can regularly be reviewed.

This is important for manufacturing companies that employ contract workers or have permanent employees requiring temporary access to systems due to being assigned to short-term projects.

Without scheduled re-certification:

- Over time, employees would acquire a greater amout of access rights than needed which could result in significant risk if their accounts are compromised
- Contractors could have on-going access to internal resources long after they have finished working with the company

However, with scheduled re-certification in place, manufacturing companies can be confident that employees and temporary workers are granted access to the resources they need to do their jobs for the period required and no more.

While access certification has traditionally not been a high priority for manufacturing companies, it is becoming increasingly important as it is being demanded by auditors as a way to ensure better governance.

Workflow

To make the management of identities as efficient as possible, it is important to have well-defined workflows that route approvals through the various processes involved in Identity Access Management and Access Governance. Most solutions available have standard templates included which include the most common processes such as when employees are initially employed, move department or location, and leave the company. These templates save administrators time when setting up common processes.

Workflows are typically displayed in a web interface which allows users to approve or reject them as well as see any of their history. Functionality such as notifications via email, escalation, and delegation are also essential to ensure that the business-critical aspects of manufacturing are not held up due to approvals not being processed promptly.

Policy and Role Management

The following areas of Identity Management and Access Governance solutions are governed by policies to determine actions that need to be taken:

- Access
- Provisioning and fulfillment
- Workflows
- Operational management
- Security
- Audit

Segregation of Duties (SoD):
Internal controls designed to prevent fraudulent activity and human error by requiring more than one person to complete a business task.

Identity and access management solutions allow companies to enforce SoD via the creation of policies preventing access to toxic combinations of access (e.g. being able to set up a supplier and make a payment to them).

Actions associated with policy management could include allowing a policy, creating an approval process for a policy, removing access entitlements for a user when a policy is no longer valid, and determining who can request specific access. Manufacturing companies should ensure that any solution they consider deploying has policies that can be defined based on rules, roles, or defined workflows as automation via policy-based provisioning can introduce significant efficiencies.

Simplifying Policy Management using Roles

Managing access rights that govern who has access to parts of the different systems under management can become complex due to high numbers of users and business systems as well as frequently changing access requirements.

To reduce the potentially very high number of user-entitlement settings that need to be made, user roles should be defined. Examples of role groups include:

- All employees based on the factory floor
- All production engineers
- All employees involved in the design of “Project Alpha”

By creating these types of roles, administrators significantly reduce the burden of defining multiple access rights for each user across all the business systems. Instead, policies will be defined for a role which will be inherited by users when it is assigned to them.

Roles make defining access rights for users quicker, easier and less prone to human error as administrators do not need to repeatedly set up the same rights for different users. Roles also mean that changes in the business environment such as mergers and acquisitions, implementations of new business systems, or the creation of temporary project teams can be managed in fewer steps rather than requiring the reconfiguration of many different user accounts.

Segregation of Duties

While it is not always a key priority compared to other requirements listed when deploying an Identity Governance and Access Management solution, Identity Management Professionals should consider setting up segregation of duty (SoD) rules to improve overall governance. If SoD is being considered, then care should be taken by administrators when setting up roles to ensure that users are restricted from having a toxic combination of access which is not permitted by the company’s business rules or regulatory requirements.

For example, a manufacturing company would not want an employee to be able to create a supplier in the purchasing system and be able to pay invoices from them as this process is open to potentially fraudulent activity.

Simplifying Role Creation

To simplify the creation of roles, some more advanced solutions have the capability of discovering the access rights that are in place for existing users across different applications. This is often referred to as “role mining”. Once access rights have been discovered, roles are automatically created by grouping users with similar requirements together. While this will not address 100% of the task of role creation, it certainly eases the administrative burden of creating roles which will in turn reduce the burden associated with user access management overall.

Reporting and Analytics

Understanding and analyzing the overall activities and access controls is an important part of ensuring that identity governance controls are effective. Reporting and analytics are used to show a detailed audit trail of who had access to what and when. Reports should be in the form of standard reports showing details over time such as user lifecycles as well as access certifications and requests and should be customizable to meet individual business requirements.

Using the reporting and analytics capabilities of an Identity Management and Access Governance solution should allow companies to significantly reduce the amount of effort required to get an overall picture of individual’s access across applications and systems. These features should also allow administrators to perform forensic analysis and to provide relevant information to satisfy internal and external audits quickly.

5. Conclusion

The areas covered in this ebook enables the organization to address common challenges revolving around efficiently working with the complex ecosystems that manufacturers deal with to design, manufacture, and sell their products. A mature IGA solution enables the organization to meet the demands of regulatory requirements that need to be adhered to do business legally. In addition, the automated processes for governance reporting and auditing minimize the risks related to migration of business-critical systems to the cloud. Automating user administration processes, implementing integrated identity management and access governance enables the organization to provide day-one access for employees, contractors, and customers, free up resources in the IT department, and continuously maintain compliance.

These challenges can be addressed through the implementation of an advanced Identity Management and Access Governance solution. Omada offers Identity Management and Access Governance solutions that specifically address the challenges discussed in this report. Omada enables organizations to achieve compliance, reduce risk exposure, and maximize efficiency – providing policies, processes, and solutions for fulfillment of governance demands.

To learn more about how Omada helps manufacturers deploy Identity Management and Access Governance to increase your IT efficiency, security and compliance please visit www.omada.net or contact your local office.

Omada

Since 2000, Omada has focused on using identity to create business value. Identity, managed the Omada way, simultaneously improves security, efficiency, cost control and regulatory compliance. And, it can do even more. Identity can accelerate digital transformations, smooth M&A integration, and enable deeper relationships with suppliers and customers. Few technologies have the potential to impact so much. Belief in this essential role of identity unites our organization, fuels our innovation, and strengthens our collaboration with partners. We have pioneered many of the best-practices in use today, and are passionate about taking identity management even further. We are committed to using identity to create business value. Omada has operations in North America and Europe, delivering solutions directly and via a network of skilled partners and system integrators.

Contact Omada

Headquartered in Copenhagen, we have a widespread partner network across Europe, North America and Africa, and sales offices in the following cities:

Omada A/S | Østerbrogade 135 | DK-2100 Copenhagen | Denmark
Omada Solutions Ltd.| 120 Pall Mall | London SW1Y 5EA | United Kingdom
Omada GmbH | Bad Nauheimer Straße 4 | D-64289 Darmstadt | Germany
Omada | Postępu 17A | 02-676 Warszawa | Poland
Omada Solutions Inc. | 530 Lytton Avenue | Palo Alto, CA 94301 | USA
Omada Solutions Inc | 413 Stuart Circle Suite 318 | Richmond, VA 2320 | USA

www.omada.net | info@omada.net

DO MORE WITH IDENTITY