WHITEPAPER

Unified Access Management: A New Identity Approach for Manufacturers

Content

Top 4 Manufacturing Challenges

What to Look for in a Solution

A New Approach:
Unified Access Management

Conclusion

About One Login

Contemporary manufacturing organizations face the challenges of globalization, fierce competition, and declining margins. As part of a greater digital transformation strategy, manufacturers are looking to improve agility across their supply chains, improve security, and simplify identity management—all at a reduced cost.

Digital transformation can be accomplished with SaaS tools, which give users the ability to work and collaborate from anywhere at any time. However, many manufacturers are still stuck utilizing commercial off-the-shelf, and custom web apps hosted on-premises, at remote data centers, and in private clouds.

The combination of all of these SaaS and legacy tools forces manufacturing organizations to manage access to distinct environments, networks, and devices separately. Here are the top 4 challenges manufacturers face as a result of this fragmented approach.

Top 4 Manufacturing Challenges

Inefficiency across the supply chain

A recent study by Aberdeen Group based on data from more than 17,000 manufacturing enterprises estimates that roughly **one in three manufacturers provide third-party access to more than 25 organizations.**[1] Moreover, about one in ten work with more than 200 external partners.[2]

Interacting with so many vendors across a complex supply chain can be a slow, manual process made even more sluggish by dependencies on antiquated tools and systems—especially on-premises applications like SAP or Oracle. All of this translates to lost productivity, and by extension, lost competitive advantage.

At-risk sensitive data

Manufacturers handle a wealth of sensitive data, including blueprints, schematics, business plans, financials, partner agreements, NPI documentation, and M&A data. Aberdeen Group estimates that manufacturers are **47% likely to experience some kind of data breach**, the fiscal impact of each ranging **between $190K and $450K each**.[3]

[1] *Manufacturing's Not-So-Little Identity Problem, Aberdeen Group, January 2018*
[2] *Ibid*
[3] *Ibid*

According to the Verizon 2017 Data Breach Investigations Report, **81% of manufacturing data breaches involve weak, stolen, or compromised user credentials**.[4] Manufacturers must also be on high alert for phishing attacks, as they face a higher volume of this type of threat than any other industry.[5]

High costs and lost productivity

Manufacturers are under constant pressure to reduce costs. They are often bogged down by the high operational costs of traditional identity management and the sluggish pace of app rollouts. Manufacturers also often face high attrition, which means IT is spending countless hours each year onboarding and offboarding employees.

End users often forget their app passwords, which not only causes delays in user productivity but slows down IT with a consistent flow of password-reset tickets. According to a recent TEI Report from Forrester, a typical organization may submit more than 4,000 reset tickets each year at a cost of $25 per ticket.[6] The result is a total cost of **more than $100,000 annually** for password resets alone.

According to a recent TEI Report from Forrester, a typical organization may submit more than 4,000 reset tickets each year at a cost of $25 per ticket.6 The result is a total cost of more than $100,000 annually for password resets alone.

Overly complex identity management

Manufacturing organizations are made up of a lot of moving parts; supply chain partners and vendors working out of various locations make for very structurally complex systems with high operational risk. In fact, Aberdeen asserts that “status quo” identity management has a median operational impact of at about **$3.5M for manufacturers, with a 10% likelihood of it exceeding tens of millions of dollars**.[7]

A major contributor to this complexity is that many manufacturers leverage both SaaS apps like Workday, ServiceNow, and ADP in addition to their own on-prem applications. This often results in several disparate directories, complicated app rollouts, and an overly complicated identity management system as a whole.

[4] *2017 Verizon Data Breach Investigations Report, Verizon, December 2017*
[5] *Ibid*
[6] *Forrester Total Economic Impact™ of OneLogin, Forrester Research, January 2016*
[7] *Manufacturing’s Not-So-Little Identity Problem, Aberdeen Group, January 2018*

COMMON APP ECOSYSTEMS

Demand Planning & ERP	Manage demand and enterprise resource planning to optimize manufacturing efficiency and costs	ORACLE	SAP	PLEX
CPQ & Procurement	Efficiently deliver Configure/Price/Quote and coordinate online procurement/EDI	SAP Ariba	APTTUS	ORACLE
Shipping & Fullfillment	Receiving and shipping logistics across the entire supply chain	UNITED STATES POSTAL SERVICE	ups	FedEx
Workflow & IT Infrastructure	Design environment and core IT infrastructure, netowrking and security	Microsoft Azure	AUTODESK	paloalto NETWORKS
Business Operations	Core business applications and services that enable the connected workforce	Office 365	ADP	G Suite

What to Look for in a Solution

Manufacturers require an affordable solution that cuts down the costs, risk, and complexity that come with managing several app permissions across several users.

IT needs a tool that empowers them to roll out any application in minutes instead of days, as well as seamlessly manage user access across both on-prem and SaaS apps. To keep sensitive corporate data secure, IT teams need a solution that offers a wide range of security options, including MFA. They also need to be able to rapidly onboard and offboard employees to keep up with high levels of attrition and keep sensitive data out of the hands of former employees.

Users need a single pane of glass through which they can securely access all applications - both SaaS and on-prem - with a single click. They should also be empowered to reset their own passwords so that IT isn't overwhelmed by helpdesk tickets, and can focus on higher priority tasks.

This is where the OneLogin Unified Access Management Platform comes in.

Manufacturers require an affordable solution that cuts down the costs, risk, and complexity that come with managing several app permissions across several users.

A New Approach: Unified Access Management

Unified Access Management (UAM) is an innovative approach that centralizes both SaaS and on-premises application environments. UAM extends access management to networks and devices using SaaS infrastructure, which unifies all corporate users and user directories.

In doing so, Unified Access Management dramatically simplifies the overall administration experience, reduces costs and operational complexity considerably, improves the end-user experience, and improves organizational security.

The OneLogin UAM solution addresses the most significant manufacturing challenges in the following ways:

Improving efficiency

OneLogin frees up time for both users and IT admins with automation and self-service capabilities. Admins can automate processes like user onboarding and offboarding, cutting the timelines for these tasks from hours to minutes. This not only means that IT's time is spared, but new employees can start being productive on day one.

OneLogin also extends secure access to users operating outside the walls of your organization. Remote employees, partners, and vendors can instantly gain the appropriate level of access to more than 5,000 pre-integrated apps like SAP, Oracle, G Suite, and Office 365.

The result is that manufacturers can more seamlessly work with vendors for a more efficient, scalable supply chain.

OneLogin also extends secure access to users operating outside the walls of your organization. Remote employees, partners, and vendors can instantly gain the appropriate level of access to more than 5,000 pre-integrated apps like SAP, Oracle, G Suite, and Office 365.

> "OneLogin enables us to roll-out more SaaS applications to the organisation efficiently and with ease. Without the tight role-based access control OneLogin affords us, it would be pretty much impossible for us to adopt any of these solutions successfully."
>
> –Jeremy Hyland, *Interim IT Director at Consort Medical*

Securing at-risk data

OneLogin comes equipped with several security tools to help manufacturers secure documents like blueprints, schematics, business plans, and financials. These tools can be applied across an organization's entire app portfolio and the entire employee lifecycle.

For example, OneLogin is built around the principle of "least privileged access." IT admins have full control over not only which users have access to which apps, but also the degree of access that each user is granted for each application. Moreover, should an employee leave the organization, IT admins can revoke access to all of their apps with a single click.

Single Sign-On enhances security by eliminating the need for employees to write down or reuse passwords for multiple accounts. And OneLogin's smart multi-factor authentication tool, adaptive authentication, scales across all apps. This tool assesses the risk-level of logins for both SaaS and on-prem apps and responds with an MFA prompt as necessary.

OneLogin also seamlessly integrates with security tools like Cloud Access Security Brokers (CASB's) and Security Information and Event Management (SIEM) solutions to add additional layers of security after logins take place.

Cutting costs and enhancing productivity

OneLogin is a dream for any manufacturing organization looking to boost both user and IT productivity. Single Sign-On grants users a single pane of glass through which they can access all apps with a single click. They do not need to remember multiple complex passwords, which means less time retyping or resetting passwords, and more time being productive.

And if users do forget their password, they have the power to reset it themselves without bogging down IT with helpdesk tickets. Users can even set up their own MFA devices, which means IT admins can spend their time working on more pressing tasks.

> "The high-level results from using OneLogin include reducing administrative costs, protecting and leveraging existing investments, time savings for IT and users, high user adoption, and providing a holistic view of security."
>
> –Nate Hauenstein, *Enterprise Infrastructure Manager at Chart Industries*

OneLogin Access takes the complexity out of identity management by offering IT admins the power to manage user access to SaaS apps, commercial off-the-shelf apps, and custom web apps hosted on-premises, at remote data centers, and in private clouds.

Reducing complexity in identity management

OneLogin Access takes the complexity out of identity management by offering IT admins the power to manage user access to SaaS apps, commercial off-the-shelf apps, and custom web apps hosted on-premises, at remote data centers, and in private clouds.

OneLogin also offers strong integration between multiple directories like Active Directory, LDAP, and HR Identity solutions. OneLogin offers real-time, Bi-directional synchronization of users, their attributes, and their groups between these sources, and merges them into a single, unified cloud directory. When a user changes positions, transitions to another department, or moves to a new office, attributes like app access, permissions, and salary are automatically updated across each of these directories.

The result is that manufacturers can not only operate with a simple identity management system internally but can also seamlessly collaborate with supply chain partners and vendors from around the globe.

> "If you need to be able to access all of your work, your data, your applications - no matter what device you're on or where you're at - OneLogin allows that to happen seamlessly."
>
> –Gary Graeff, *IT Group Manager at Steelcase*

OneLogin's focus on access unification, automation, and security means that IT admins can check all of these boxes at a reduced cost. As a result, manufacturers reap the rewards of improved agility across their supply chains, optimized security, and a simplified method for identity management.

Conclusion

Let's recap what we've learned.

Manufacturers are looking to embrace digital transformation to stay competitive, but face the challenges of high costs, inefficiency, complexity, and risk caused by disparate application portfolios including both cloud and on-premises applications.

IT Admins need a solution that offers simple, unified access management to each of these applications for all users. This solution must be able to keep up with the rapid onboarding and offboarding of employees in the manufacturing sector and provide additional layers of security like MFA, SIEM, and CASB integrations.

End users need a single intuitive pane of glass through which they can securely access all of their apps. And they require self-service capabilities so that they are empowered to reset their own passwords when needed.

OneLogin's focus on access unification, automation, and security means that IT admins can check all of these boxes at a reduced cost. As a result, manufacturers reap the rewards of improved agility across their supply chains, optimized security, and a simplified method for identity management.

See if OneLogin is a fit for your organization. Get your personalized demo.

About OneLogin, Inc.

OneLogin is the leader in Unified Access Management, Enabling Organizations to Access the World™. OneLogin makes it simpler and safer for organizations to access the apps and data they need anytime, everywhere. The OneLogin Unified Access Management Platform secures millions of identities for thousands of companies around the globe, spans both cloud and on-prem environments, and unifies all users, devices, and applications to transform enterprises. We are headquartered in San Francisco, California. For more information, visit www.onelogin.com, or connect with us on our blog, Facebook, Twitter, or LinkedIn.