DIGITAL IDENTITY SOLUTIONS FOR MANUFACTURING

WHITE PAPER

TABLE OF CONTENTS

INTRODUCTION

As a manufacturer, you face a number of new challenges and shifting priorities. Evolving and emerging trends have changed the way you operate and conduct business. Chief among these trends is globalization.

You're probably familiar with the saying that a supply chain is only as strong as its weakest link. Globally distributed manufacturing creates a complex network of relationships. This complexity can make it more difficult than ever to identify where your weak links exist. There's no choice but to keep moving forward, yet there's also no denying that you're at increased risk.

These risks aren't limited to the assembly line either. Globalization requires providing a range of users—from employees to partners to suppliers—access to the resources and applications they need to do their jobs.

The flip side of providing access to authorized users is keeping unauthorized users out. Because a manufacturer's intellectual property and trade secrets are among its most valuable assets, their enterprises are popular targets for both internal and external bad actors.

"73% of manufacturing breaches began at the identity level."[1]

The unfortunate reality is that the same advances that have fueled manufacturing growth have also made your attack surface larger and more challenging to secure. IT is tasked with enabling secure access and managing the associated risks, while simultaneously delivering on directives to improve efficiency, increase productivity and speed time to value. Suffice it to say, you have a lot to juggle and may be facing increased costs and inefficiencies across your enterprise.

But you have a way to keep all of those balls in the air. Cloud computing holds the promise of hope. You can leverage the power and scalability of cloud computing to innovate, reduce costs and gain a competitive edge across all areas of your business. And you don't need to be one of the big players to get in the game.

Read on to learn more about how the Ping Identity Platform can help you navigate a successful migration.

1 2017 Data Breach Investigations Report, Verizon, Apr 27, 2017.

MANAGING GLOBALLY DISTRIBUTED ECOSYSTEMS

Globalization has presented many benefits to manufacturers. The ability to control labor costs, improve access to raw materials, accomodate an increasingly global customer base and expand to new markets have driven both top and bottom line improvements.

Globalization has also presented challenges for IT teams specifically. Chief among these is managing resource access for employees, partners and suppliers spread across the globe. Add mergers and acquisitions to the equation, and the scale and complexity of these challenges is compounded.

An IAM solution, like the Ping Identity Platform, enables you to give the right users secure access to the right resources. Beyond these fundamentals, it helps you deliver a unified end-user experience and operate as a cohesive, digital entity, regardless of where your infrastructure, networks or facilities may exist across the globe.

ENABLING SEAMLESS GLOBAL ACCESS

As your business expands globally, you must manage access not only for different types of users, but from different regions and unfamiliar networks. Likewise, the applications your users are trying to access are often located in various regions and networks, too.

Granting access is just the beginning. In the digital age, where a user could be managing as many as 191 passwords[2], you also want to enable single sign-on (SSO). This capability gives your users a one-stop sign-on experience.They sign on just once using a single set of secure corporate credentials and gain one-click access to all their applications from anywhere.

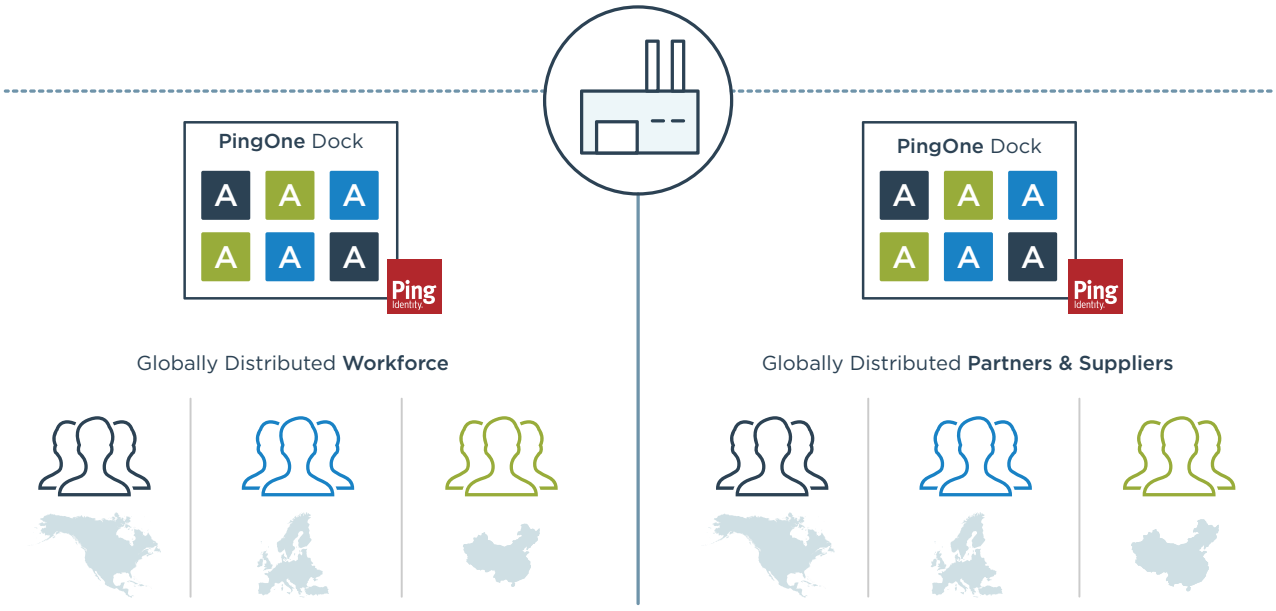

Figure 1: Ping Identity grants users one-click access despite user, network or app location.

2 "The Password Expose: 8 truths about the threats – and opportunities – of employee passwords," LogMeIn, Inc., Nov 2017.

LEVERAGING IAM FOR A GLOBAL WORKFORCE

The consumerization of IT isn't a new concept. Today's employees are also today's consumers. They expect the same type of user experience from their employers as they receive from their favorite retailers.

When your employees aren't able to access the applications they need, the impact is felt across the business. Decreased efficiency, lowered productivity and a subsequent increase in helpdesk requests are often the rule instead of the exception.

Providing seamless and secure access to all on-premises, cloud and SaaS applications is step one. You want to enable self-sufficiency to manage the IT burden and manage password sprawl to mitigate security risks.

The Ping Identity Platform's SSO solution allows you to do both. You're able to provide your employees with a cloud-based dock, accessible from any location or device. Administered from a centralized interface, Ping's SSO solution enables federated single sign-on from managed devices to mobile, cloud and enterprise applications. The addition of multi-factor authentication (MFA) steps up security based on risk, giving you increased assurance that employees are who they say they are.

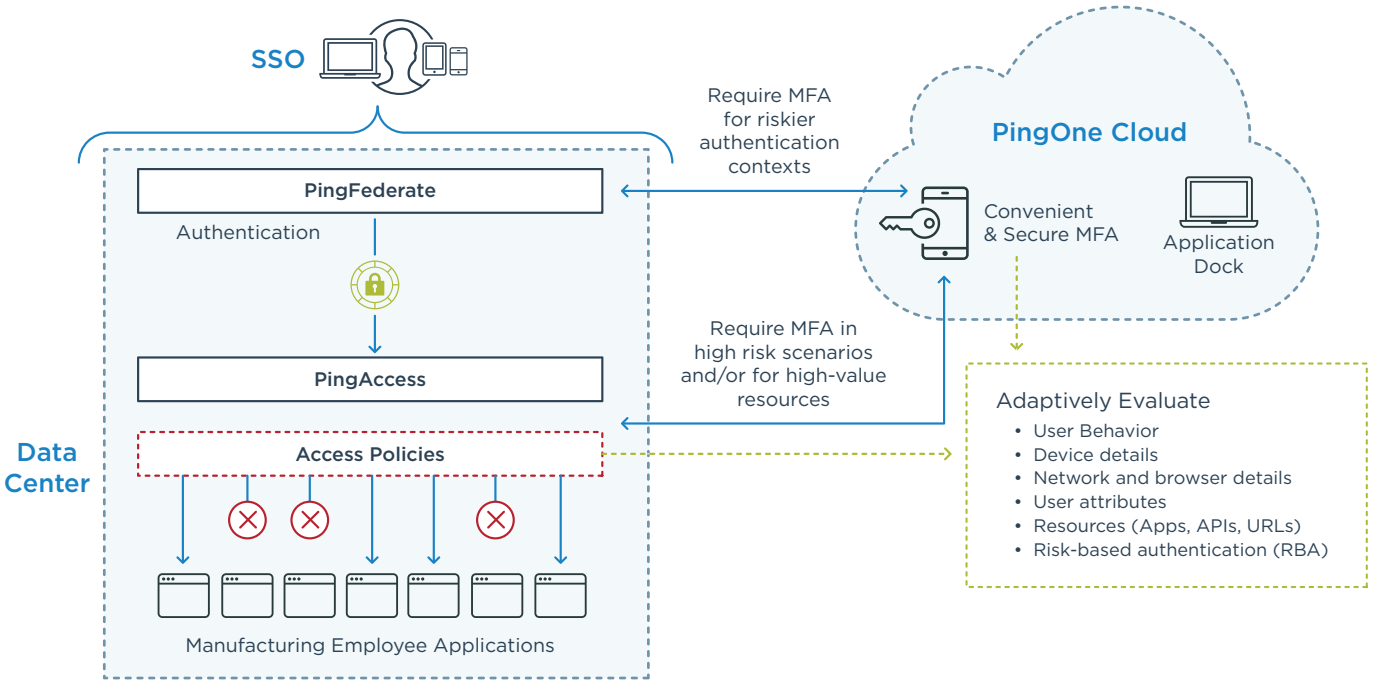

Figure 2: Enable adaptive MFA to grant employees seamless, secure access.

LEVERAGING IAM FOR GLOBAL SUPPLY CHAIN PARTNERS

Large manufacturing enterprises may have tens of thousands of partners and suppliers who need to access applications. These might include logistics or inventory applications, design applications or project management software. Further, these partners and suppliers have diverse characteristics, varying in location, size, technical capabilities and more.

You need an IAM solution that provides flexibility to enable secure access for this diverse user population. The Ping Identity Platform gives you options to grant seamless access to suppliers large and small:

- You can leverage a simple cloud directory to provide access to a smaller or less-sophisticated partner.
- For partners and suppliers with their own directories, you can bridge an existing directory or directly connect to their directory.

You also want to avoid taking on the management of your partners' and suppliers' employee identities. Giving responsibility to your partners for managing their own identities provides greater assurance that only current and authorized employees have access, which in turn minimizes your risk of breach.

With the Ping Identity Platform, identity onboarding, management and de-provisioning can be delegated to the partner or supplier organization. This frees up your IT resources to focus on higher value activities.

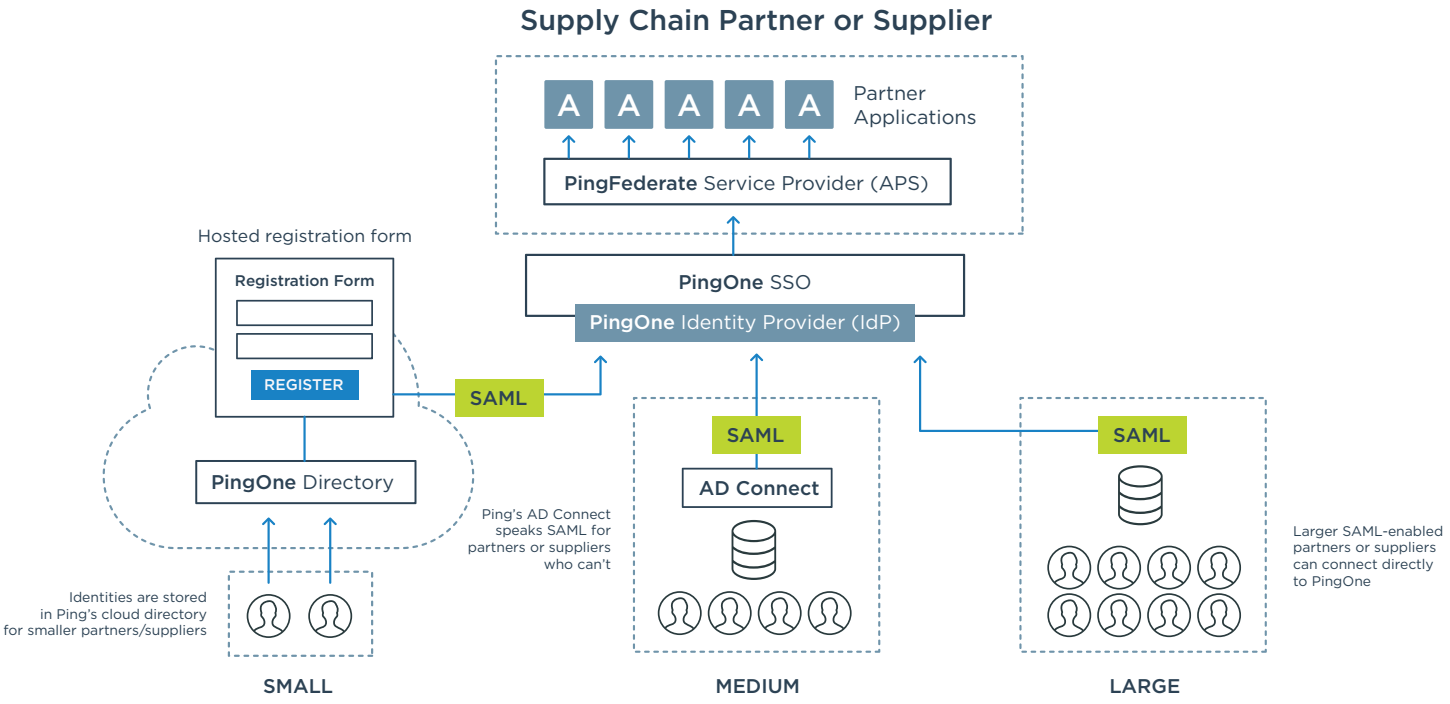

Figure 3: The Ping Identity Platform enables you to grant secure access to partners and suppliers, regardless of their technical capabilities.

FACILITATING INTEGRATION OF MERGERS & ACQUISITIONS

Globalization isn't limited to organic growth. It often comes in the form of mergers and acquisitions. But the rationalization and integration of disparate IT infrastructures can slow the time to value of these significant investments in growth.

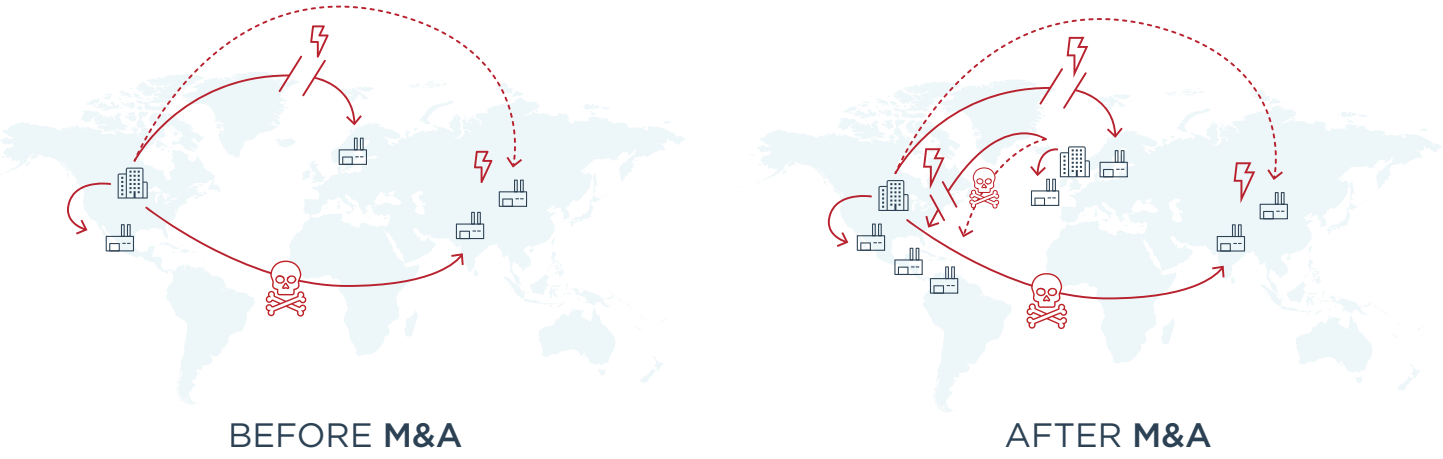

Figure 4: M&A adds scale and complexity to your globalization challenges.

Built on open standards, Ping Identity's enterprise-grade platform simplifies the connecting of disparate data sources to a single authentication authority. Supported with out-of-the-box integrations, token translators and connectors, you're able to accelerate integration, and in doing so, accelerate the time to value of your merger or acquisition.

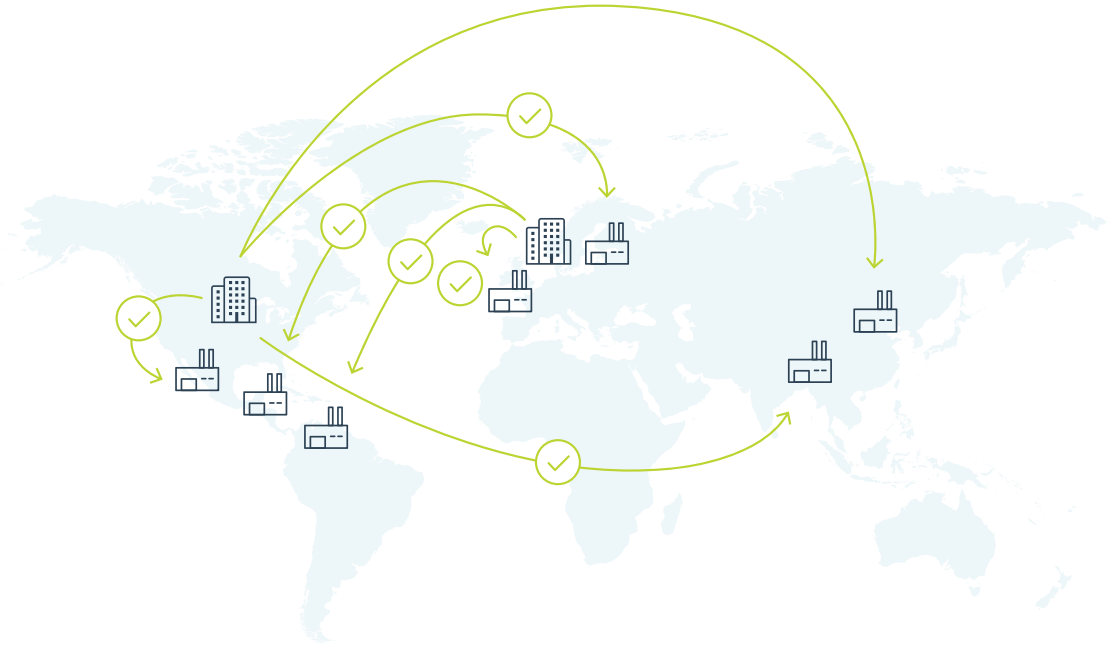

Figure 5: The Ping Identity platform accelerates integraton by connecting disparate data sources to a single authentication authority.

SECURING INTELLECTUAL PROPERTY & TRADE SECRETS

As a manufacturing company, you possess proprietary data and information that isn't just highly valuable to you, but pretty attractive to attackers, too. Your threats include competitors, opportunistic hackers, even nation states and your own employees.

When your applications and employees can't be bound by a firewall, a perimeter-based security model no longer works. You need a modern approach to enterprise security. Identity-centered security can help you keep your most valuable information secure.

MOVING PAST THE PERIMETER TO INDIVIDUAL IDENTITIES

Your intellectual property is one of your most valuable assets, making it a prime target for bad actors, both inside and outside your enterprise. If you have facilities in other countries and across many networks, you're at greater risk. Globalization as a whole has increased the surface area for potential attacks. This is only compounded by a mobile workforce.

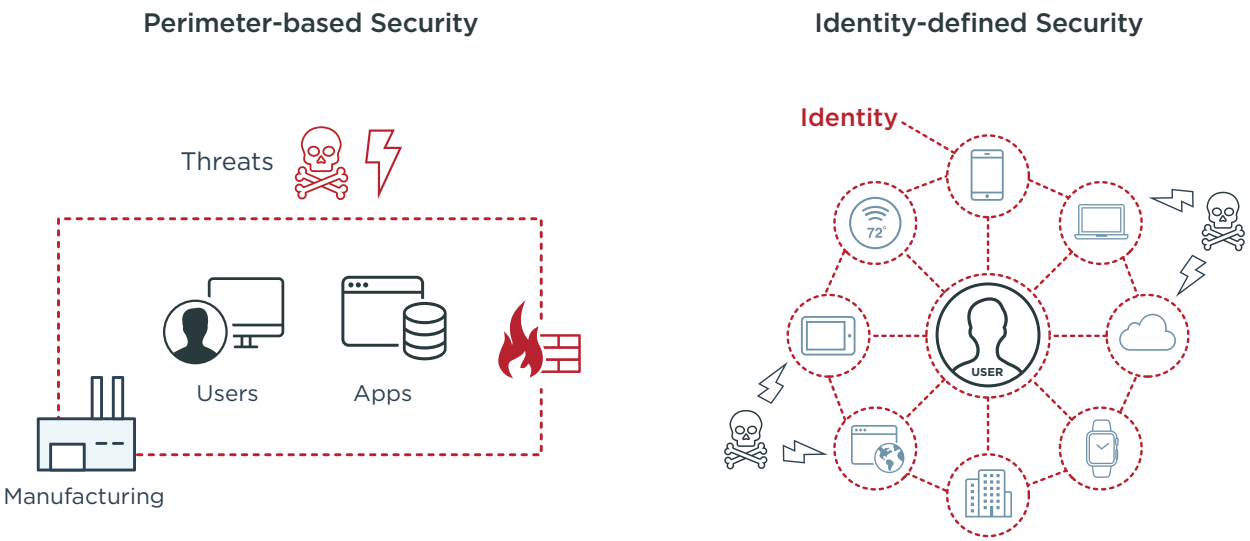

Figure 6: Outdated perimeter-defined security in contrast to modern identity-defined security.

To address security in a borderless world, you must look beyond the perimeter to the individuals seeking access. This requires a subtle but significant shift in your approach. Instead of keeping the wrong people out, you're ensuring that only the right people get in. To do this, you rely on identity.

Identity-defined security secures the individual user, enabling you to grant the right people access to the right things. The result is a more secure and agile approach to security that's perfectly suited to the challenges manufacturers face.

ENABLING SECURE ACCESS & AUTHORIZATION WITH IAM

Giving the right people access to the right things is a nuanced process. You need to make sure that users are who they claim to be, and that they're authorized to access the applications they're requesting. You want to make the sign-on and authentication processes as seamless and convenient for your users as possible, while maintaining access security over your proprietary systems and information. An enterprise-grade IAM solution helps you strike the right balance between user experience and enterprise protection.

With the Ping Identity Platform, you can enable single sign-on (SSO), so users need only one set of login credentials to access applications and resources, minimizing your attack surface. Adaptive MFA capabilities allow you to ensure users are who they say they are with minimal friction and enhanced security. Access security allows for even finer-grained policy controls that enable you to manage whether a user is authorized to manage a given resource. Meanwhile, a robust, scalable directory solution securely stores identity data and encrypts it while in transit, at rest and during replication.

AUTHENTICATE USERS ADAPTIVELY

With adaptive MFA, you require additional authentication only as needed and based on the risk associated with the transaction. You can allow users to conduct low-value transactions from trusted locations and devices without interruption, while prompting additional authentication during high-value transactions on untrusted networks and devices. Relying on a variety of risk and contextual factors customized to your business, you're able to keep employees productive and your enterprise secure.

With PingID, Ping's adaptive MFA solution, your user's trusted mobile device becomes the second authentication factor. Their sign-on triggers authentication policies that use context—such as geolocation, time of day, network and more—to complete authentication. Once the user's identity is verified, a token is issued that allows them to access the resources they need.

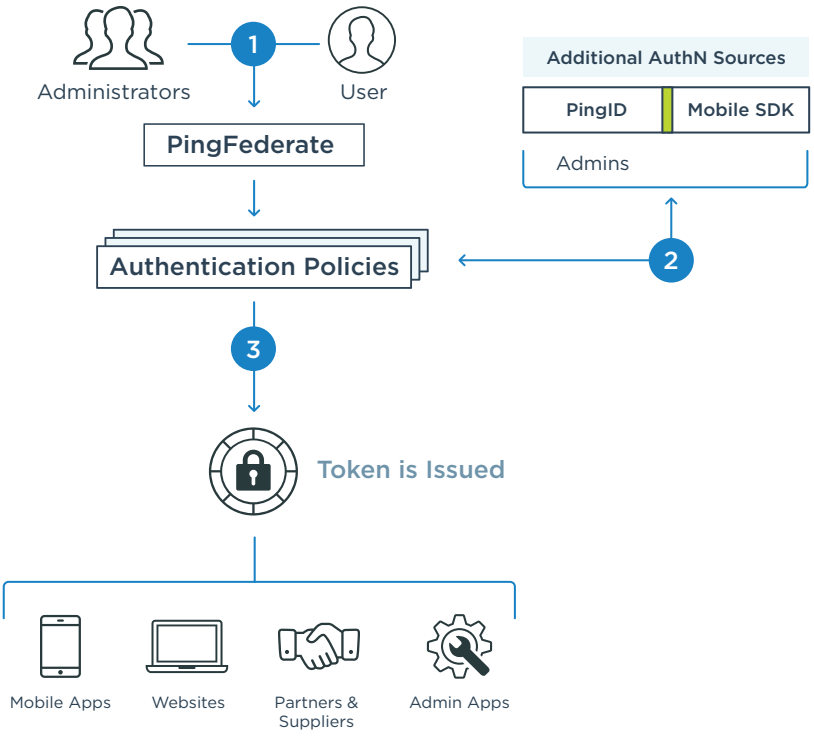

Figure 7: How the Ping Identity Platform enables adaptive MFA.

GRANT ACCESS SECURELY & SELECTIVELY

To secure access, Ping's SSO product, PingFederate, issues a token at the authentication stage and passes it to the access security solution, called PingAccess. PingAccess allows for even finer-grained controls, including URL-level access to resources so that users—a design partner, for example—only has access to the specific portion of the application they need and no more.

Further, certain applications can be set up to add additional security, such as stronger MFA requirements. Administrators can customize access policies based on user attributes such as groups, location, time or device. Once approved, access to the resource is granted. Chief among the benefits of this approach is the ability to selectively enforce security measures as needed based on the risk profile of the applications themselves.

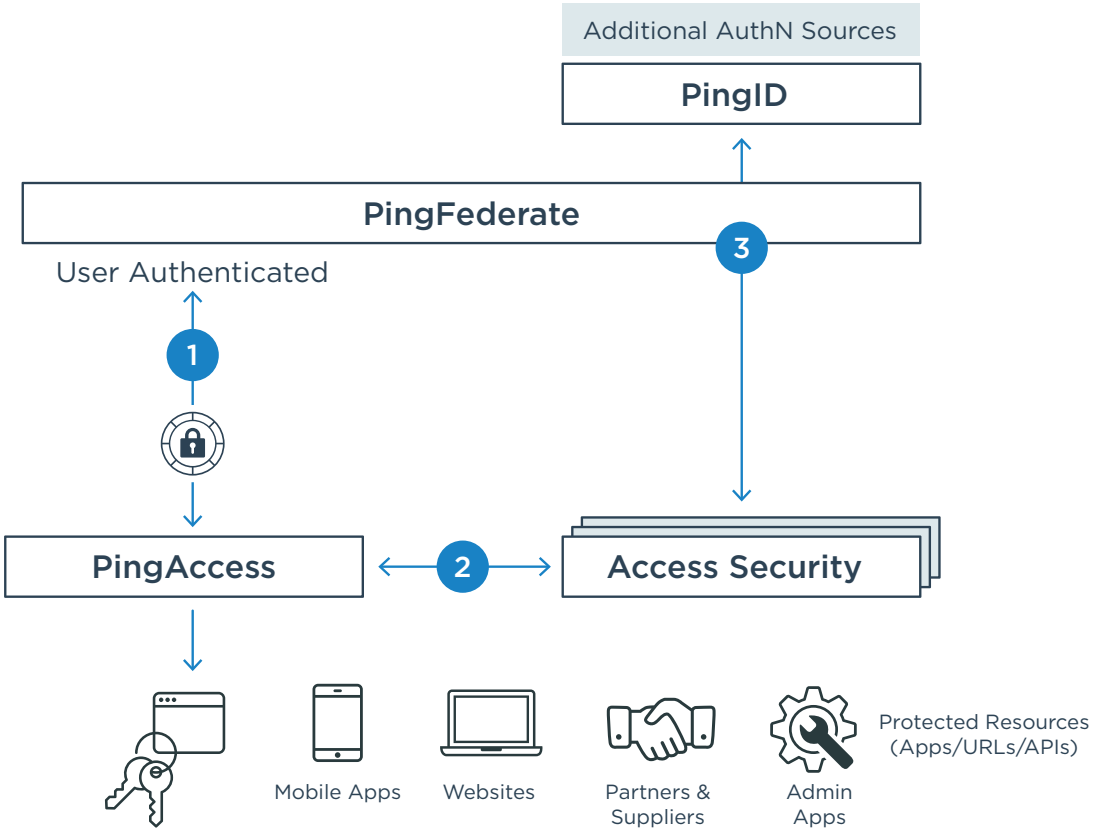

Figure 8: A common use case showing how the Ping Identity Platform enables secure access.

STORE & PROTECT DATA AT ALL STAGES

Whether you're storing employee or partner identities, it's critical to have a directory solution that's tailored for identity and profile data. Multi-purpose databases and legacy LDAP may not give you the flexibility, security or performance you need for identity management. These insufficiencies can leave you at increased risk of breach, not to mention performance lags and outages.

PingDirectory, Ping's user directory solution, securely stores identity and profile data. Offering end-to-end data encryption, it exposes identity data to applications and channels through developer-friendly REST APIs or LDAPv3. Providing performance and scalability to keep pace with your growth, PingDirectory enables faster time to market for new applications through APIs and improved security, while reducing your hardware footprint and TCO.

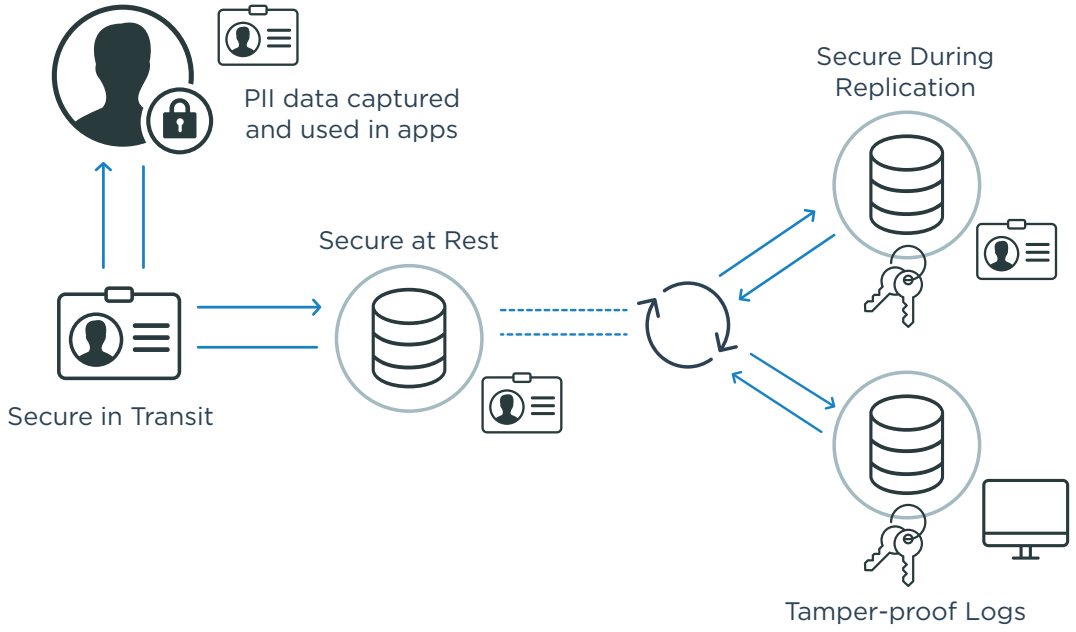

Figure 9: How PingDirectory provides end-to-end data encryption.

CUTTING COSTS & INCREASING EFFICIENCY

If you're like most manufacturers, you're competing in an extremely cost-competitive environment where accelerating time to market and lowering costs can mean big financial gains for your enterprise. Within each segment along your value chain, it is paramount that your business is running efficiently to maximize time to value and ensure that operating costs are low.

Productivity is another important part of your overall operational efficiency. In addition to optimizing throughput and lead time, you also need your employees, partners and suppliers to be performing optimally. This includes giving them seamless access to the resources they need to do their jobs.

LOWERING COSTS, WHILE INCREASING BUSINESS AGILITY

Manufacturing IT departments often face overtaxed bandwidth and overstretched budgets. To exacerbate this further, legacy IT systems are notoriously costly to operate and maintain. When you're burdened by a rigid infrastructure, you're limited in your agility and ability to implement changes and improvements.

A modern IAM solution can reduce your costs and complexity, and subsequently increase your agility. By enabling adaptive MFA, you can eliminate costly hardware tokens and instead leverage your users' devices as secure second factors. You can replace SMS and voice with mobile notifications to further reduce costs.

To go faster, you need a directory built for today's challenges. PingDirectory provides development templates so you can rapidly implement changes and new services. Modern access management further increases your agility by easing your cloud migration. You're able to control access to both cloud and legacy applications, and use capabilities like bi-directional sync for zero downtime migration.

"A modern television is built from 2,000 components, a car from 30,000 and an Airbus A380 from over 4 million. These raw materials and parts must flow in from thousands of locations to arrive across the globe on-time, on-spec and in-budget. This complex chain requires huge scalability, access by multiple devices with different operating systems and the ability to manage large pools of data, all done cost-effectively—it is difficult to imagine building this outside of a cloud network."[3]

3 Ascending Cloud: The adoption of cloud computing in five industries, The Economist Intelligence Unit, Mar 1, 2016.

INCREASING WORKFORCE & PARTNER PRODUCTIVITY

You don't want your users to endure multiple logins to access job resources, nor do you want to be swamped with password reset requests. These productivity killers are unnecessary when you rely on IAM to give the right people access to the right things.

When you provide secure SSO for your employees, partners and suppliers, you give them frictionless, one-click access to on-premises, cloud and SaaS applications. As an added bonus, you mitigate the proliferation of unsafe password practices, like relying on sticky notes to remember them all or just reusing the same password everywhere.

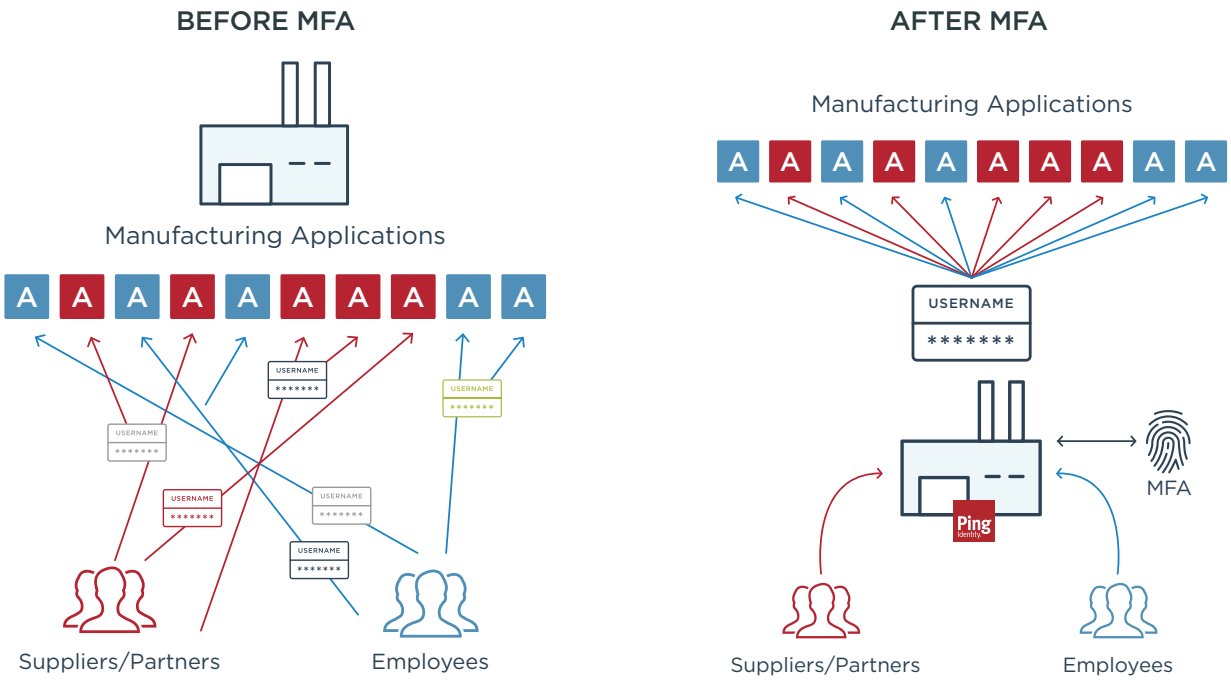

Figure 10: Before MFA, users experience several points of friction when accessing resources. After deploying MFA as part of an IAM solution, users are able to seamlessly and securely access applications, improving productivity.

MODERNIZING WITH CLOUD & HYBRID IT DEPLOYMENTS

Some industries have rushed to migrate their on-premises infrastructure, apps and data to cloud alternatives. Even the most successful cloud migrations typically involve a transition period, though. This type of hybrid environment allows enterprises to leverage new cloud apps while managing existing on-premises resources.

Because manufacturers are naturally tethered to the physical world, they'll always keep one foot on the ground or, more accurately, on-premises. A hybrid deployment, in this case, can be a permanent or long-term solution. You can use your IAM platform to give users a seamless front-end experience, regardless of where resources live on the back-end. It's a best-of-both-worlds scenario that allows you to maintain business as usual and minimize impact on your users.

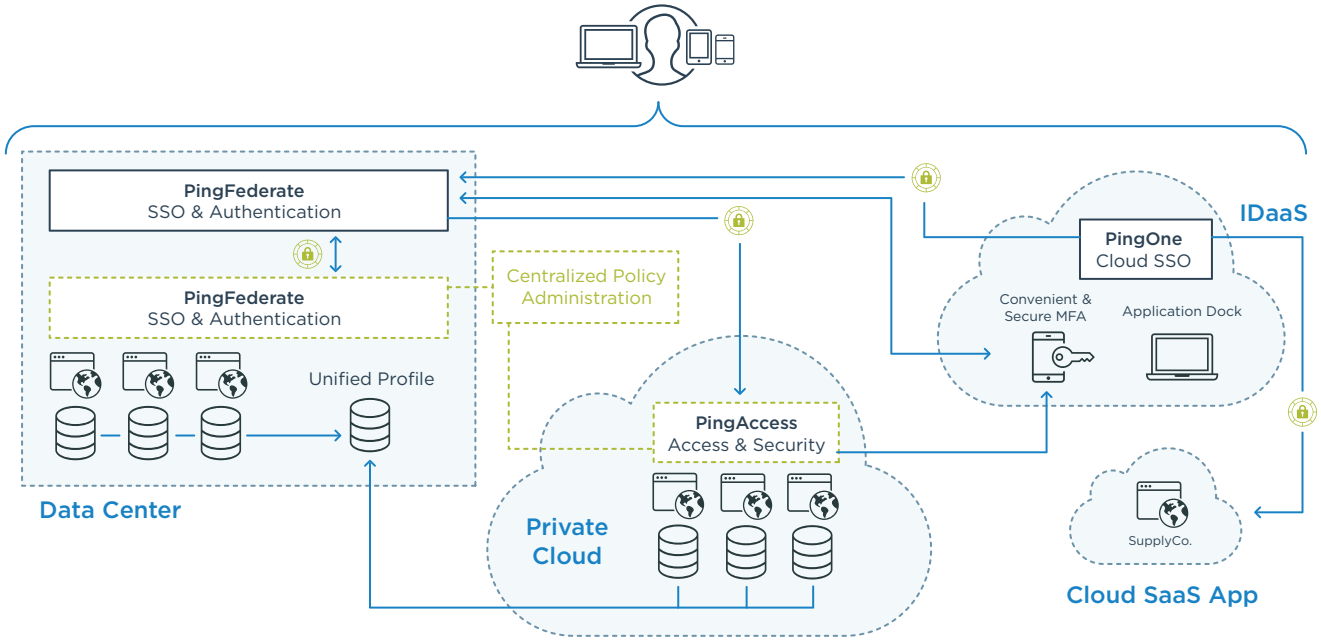

Figure 11: The Ping Identity Platform is ideal for hybrid IT environments.

The Ping Identity Platform gives you the flexibility to tailor your IAM implementation for a hybrid environment. Cloud service allows you to rapidly connect SaaS applications with IAM standards, like SAML and OpenID Connect, while an identity bridge can be deployed to rapidly connect your legacy and enterprise web applications. With almost 100 connectors and integration kits, you're able to quickly give your users secure access.

Finally, the Ping Identity Platform lets you manage IAM how and where you want. Our IAM services can be deployed on-premises, as multi-tenant IDaaS, single-tenant private cloud and managed services, or as a hybrid IT combination. You're able to meet future needs, while maintaining consistent management tools and training, all with a single IAM solution.

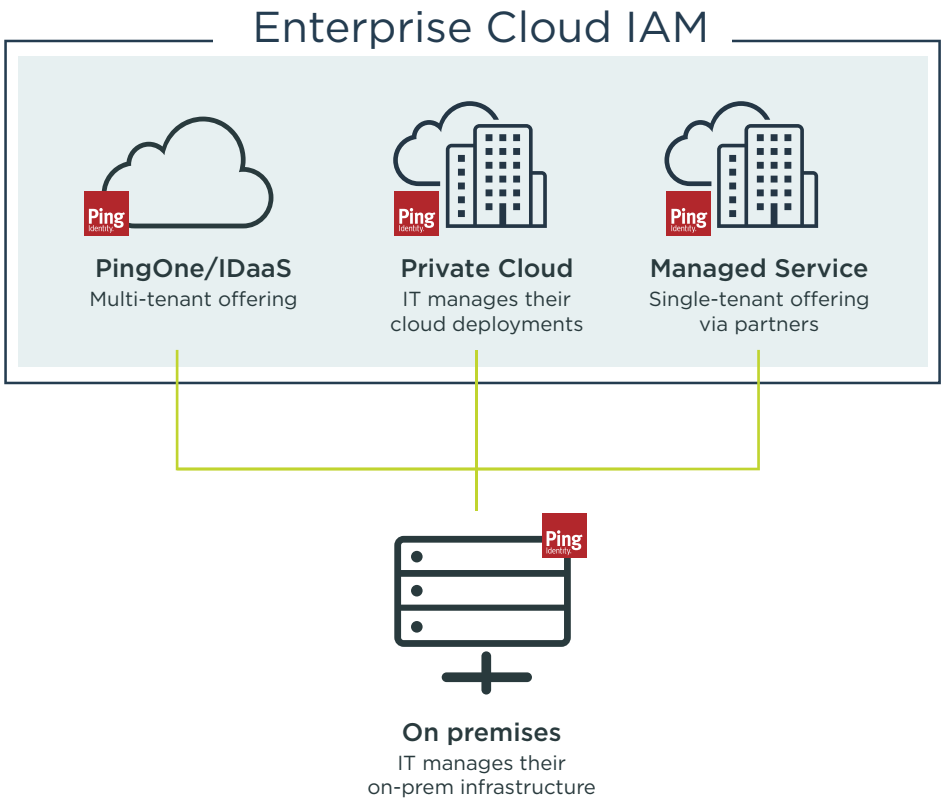

Figure 12: Enterprise cloud IAM allows you to manage how you want, where you want.

CONCLUSION

Manufacturing has become a global business. This has delivered many benefits to the industry, but has created plenty of challenges, too.

As the stakes grow larger, investment in research and development has become a key driver of competitive advantage. The possibilities are virtually unlimited for manufacturers that embrace agility and innovation. But with these opportunities come increased risks. As your intellectual property and trade secrets become more sophisticated, they also become more attractive to attackers.

Responding to the pressure to adapt or die, while maintaining a strong security posture, is no trivial task. The Ping Identity Platform enables you to respond to the unique challenges you face:

- Increase employee productivity
- Give employees, partners and suppliers secure access to resources
- Improve IT security and performance, while reducing footprint and operating costs
- Manage risk and support diverse business models

Some of the world's largest manufacturers trust Ping to help them solve these challenges. To learn how we can help you, visit www.pingidentity.com/manufacturing.

#3322 | 04.18 | v001