Manufacturing:

Securing your factories from online threats

swivelsecure

© 2019 Swivel Secure

Contents

04 Introduction

06 **Article:** Industry 4.0 and the cybersecurity risks to the future of manufacturing

12 **Infographic:** The rise of smart factories and the cybersecurity risk they pose

14 **Article:** 7 top cybersecurity tips for manufacturers

22 **FAQs:** Manufacturing cybersecurity

© 2019 Swivel Secure

Introduction

Manufacturing

Industry 4.0 has propelled the manufacturing industry through massive technological advancements in recent times. From cloud computing to automation, the manufacturing supply chain has become more connected than ever as cyber-physical systems replace older, silœd machines.

And the results have been beneficial for the industry - with these newer technologies improving efficiency, accuracy and flexibility in our factories.

However, cybersecurity regulations have been slow to catch-up and despite being the third most targeted industry, manufacturing is one of the least prepared.

Read on to find out what you can do to help protect digital technology against cyber threats.

Article

Industry 4.0 and the cybersecurity risks to the future of manufacturing

Despite being the third most targeted industry for a cyberattack, manufacturing is one of the least prepared.

Manufacturing is becoming increasingly digitised as the industry is adopting automation, to a greater extent than ever before. The Industrial Internet of Things (IIoT) is bringing artificial intelligence, cloud computing and robotics into factories. Cyber-physical systems can now integrate all aspects of the supply chain, including operational systems and information systems, and are taking the place of outdated, silœd machines.

Any factory making use of these new technologies is known as a Smart Factory, and they're prompting what experts are calling the fourth industrial revolution, or Industry 4.0. Smart Factories will help the manufacturing industry considerably, as digital technology can offer greater efficiency in the production stage, better quality products with fewer mistakes, and more flexibility for working processes.

So it's no wonder that manufacturers are moving quickly to update their factories – by 2019, 75% of large manufacturers will have incorporated the Industrial IoT in their operations. And by 2022, the Industrial IoT market is expected to be worth $19547 billion.

© 2019 Swivel Secure

The smart factory network

The devices in a Smart Factory are able to transmit data over a wireless internet connection in real time. A typical set up might include multiple systems which are accessed from a number of devices. For example, a Smart Factory might have a Product Lifecycle Management (PLM) system which can transmit design information to the Manufacturing Execution System (MES) where the product is produced. This may be controlled by a Human Machine Interface (HMI) such as a control panel or even a smart phone.

This kind of configuration allows for the seamless flow of information between machines. That information can then be used to adjust and optimise the machines' performance and achieve maximum efficiency whilst minimising waste. It also means the process can be automated, resulting in a reduced downtime which can help improve quality and reproducibility, increasing profitability.

Another advantage of the Smart Factory arrangement is that it allows for a continuous overview of the process. Through the HMI, manufacturers can have real-time visibility and access to data that provides information on the condition of machinery, remotely, provided by cloud computing capability.

Manufacturers are investing in digital

Despite the benefits they offer, the connected nature of Smart Factories leaves the manufacturing industry open to a variety of potential cyber threats – a concern which is preventing some manufacturers from completely updating their operations.

The EEF's 2018 Cybersecurity Report found that while 91% of manufacturers are investing in digital technology, 35% said they are inhibited from fully investing due to cybersecurity concerns. And it's a legitimate concern – cybersecurity is a real risk for manufacturers. The EEF report found that 24% of manufacturers admitted they have already sustained financial or other business losses as a result of a cyberattack. But with the fast-moving advancements and opportunities Industry 4.0 is delivering to manufacturers willing to invest, organisations can't afford to fall behind their competitors.

What cybersecurity risks do manufacturers face?

The result of not securing the Smart Factory network is clear. The manufacturing industry is the third most targeted industry for cybercrime, just behind the finance and government sectors. Often, attackers are looking to do one of three things through their crime:

• **Steal data** – with client details stored on CRM systems, hackers might look to take this information and hold it to ransom

This happened in 2013, when American retailer Target was the victim of a data breach that allegedly saw the theft of the personal details from between 70 and 110 million people. Attackers initially gained access through Target's heating and air conditioning supplier – the manufacturer's operational systems were hacked and due to their connection to Target's IT infrastructure, it provided a gateway for the hackers to infiltrate.

An integrated supply chain from supplier, to logistics provider and retailer means more manufacturers will have access to their client's operational systems. Attackers can exploit this connection, so manufacturers need to secure their own network to ensure the security of their clients'.

• **Disrupt access systems or operational systems** – hackers can take control of manufacturing processes to interfere with production or even tamper with the products

© 2019 Swivel Secure

American pharmaceutical company, Merck, was infected by the NotPetya cyberattack. Ransomware apparently disabled the manufacturer's email and allegedly caused mass disruption to work. It's estimated that Merck allegedly suffered a loss of over $135 million in sales, plus $175 million in additional costs.

Any disruption to production is costly for manufacturers. But incidents like the above also raise concerns about physical safety. With attackers able to infiltrate and remotely control production processes, they could tamper with products and make them unsafe, potentially harming consumers.

• **Gain intelligence for a competitive advantage** – industrial espionage sees hackers steal intellectual property or information for the advantage of competitors

In 2011, some oil production companies lost legal and financial information to a cyberattack. The motive was identified as industrial espionage, possibly to sabotage potential business deals for the companies.

Having confidential information stored on connected devices is essential. But the IoT means that information can be accessed in more ways than ever before, from laptops to smartphones or control panels. These devices offer a way for attackers to infiltrate the network and for manufacturers, increases the risk of industrial espionage.

How can the manufacturing industry mitigate risk?

While it's clear manufacturers are seeing the benefit of Smart Factories, the cyber risks they present are stalling progress. But with the proper time and financial investment in cybersecurity, the industry will be able to enjoy the full benefits of Smart Factories.

A significant lack of awareness of the importance of cybersecurity still plagues the manufacturing industry. The EEF report found 34% of manufacturers said cybersecurity dœsn't appear on their risk register. A worrying statistic considering the majority are investing in digital technology.

It's crucial that manufacturers establish cybersecurity regulations within their Smart Factory.

© 2019 Swivel Secure

Three key questions every manufacturer should ask themselves:

1. Are you investing enough in cybersecurity?

While governing bodies like the EU have begun to invest more in outlining cybersecurity standards, there's a concern that there isn't enough focus on the manufacturing industry and frameworks aren't always relevant.

There's still a lot of research to be done to identify the specific needs of manufacturers but investing in a range of security services including consultancy, training, software and hardware could help your business mature more quickly.

2. Do you have a clear response strategy to mitigate an attack?

12% of manufacturers surveyed said they had no technical or managerial measures to assess or mitigate a cyberattack. Without a proper response strategy, there's a risk that it could take longer for the business to recover and this will intensify any damage caused – financial or otherwise.

Manufacturers should have an audit trail for compliance, and cyberattack insurance in place to provide support in the event of a data breach and for mitigation purposes. There also needs to be a clear management plan to minimise the effects. It's thought that cyberattacks will only become more prevalent.

3. Can you afford to ignore the risk?

Attacks can range from causing minor production disruption to inflicting serious damage to machinery. As we've already seen how Merck allegedly lost an estimated $310 million to a breach, it's obvious that a similar attack could be crippling to a smaller company.

So while investing in cybersecurity or cloud computing security can be expensive, not doing so could be more costly in the long run.

Infographic

The rise of smart factories and the cybersecurity risk they pose

The manufacturing industry is being propelled toward Industry 4.0. With the rise of Smart Factories, we're seeing advanced digital technology and automation become a familiar feature of the supply chain. The effects promise to be beneficial for manufacturers – automation can help improve efficiency and accuracy while reducing mistakes and waste.

But, the connected nature of Smart Factories can also leave manufacturers open to a greater risk of cyberattacks. So it's crucial to ensure any manufacturing systems are protected to minimise the risk of unauthorised access.

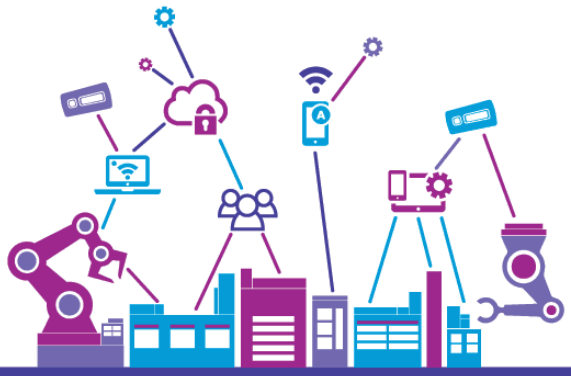
Take a look at our infographic to learn more about the state of Smart Factories, and how to manage the risk they pose.

© 2019 Swivel Secure

The rise of smart factories and the cybersecurity risk they pose

The rise of smart factories will help the manufacturing industry considerably, as digital technology such as automation can lead to greater efficiency and accurate reproducibility, leading to optimum product quality with minimum waste.

But, these connected devices expose a greater risk for hackers to remotely attack all aspects of the supply chain. As these threats increase, manufacturers need to ensure they are protecting their systems in the correct way to minimise unauthorised access.



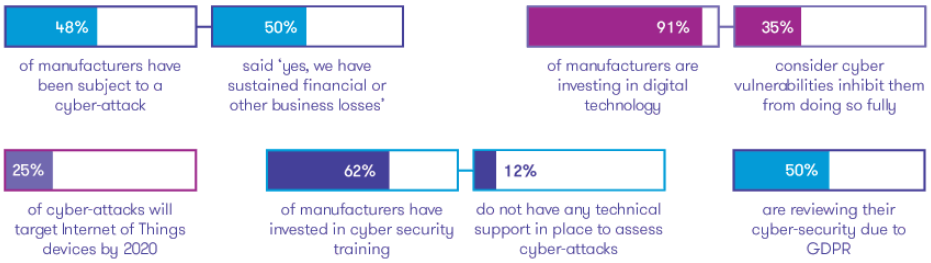
The future of the factory

Digital transformation trends in manufacturing

- IoT & Industry 4.0
- AI & machine learning
- Robots
- Improved efficiency
- Data and analytics

Smart factory adoption per industry by 2020:

The risks...



Risk management

MFA

can be used to protect applications such as ERP systems and to protect your CRM

Jump host

can be protected with MFA onto the control network

This will separate MES from PLM and ERP

ISO 27000

series of security standards have been issued to help businesses manage their data assets

Sources:

Information Age. 2018. The Internet of Things: The security crisis of 2018. [ONLINE] Available at: https://www.information-age.com/internet-things-security-crisis-123470475/

Moschip. 2018. Smart Factories Infographic. [ONLINE] Available at: https://moschip.com/wp-content/uploads/2018/05/Smart-Factories-infographics-final-1.jpg

EEF. 2018. Cyber Security for Manufacturing. [ONLINE] Available at: https://www.eef.org.uk/resources-and-knowledge/research-and-intelligence/industry-reports/cyber-security-for-manufacturers

Forbes. 2017. Top 5 Digital Transformation Trends in Manufacturing. [ONLINE] Available at: https://www.forbes.com/sites/danielnewman/2017/08/08/top-5-digital-transformation-trends-in-manufacturing

Abbreviation Glossary:

MFA: Multi-factor authentication - a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login.

ERP: Enterprise resource planning

MES: Manufacturing execution system

PLM: Product lifecycle management

swivelsecure

www.swivelsecure.com

Article

7 top cybersecurity tips for manufacturers

Cybersecurity has become a government priority, but the manufacturing industry is falling behind commercial business. The last few decades have seen numerous incidents where sensitive data has been compromised. Consumer information like email addresses, banking details and passwords have been stolen and used by hackers for a range of crimes including fraud and blackmail. One of the most widely reported incidents occurred recently, with the security of an estimated 50 million Facebook accounts attacked, seriously breaching users' right to privacy.

The introduction of GDPR

Incidents like this led to governing bodies working to formalise data protection laws. In May 2018, GDPR was implemented and affects all data for individuals within the EU. It aims to give people better control over their personal data and holds businesses to account for any mishandling of their customers' information.

As a result, we've seen commercial businesses such as retailers tighten their data regulations and clarify how they use, maintain and store customer information. The supply chain is becoming ever more digitally connected, and it's likely that some original equipment manufacturers (OEM) in the B2C sector will have direct access to personal customer data for warranty purposes, while manufacturers in the B2B sector are likely to have access to customer data via CRMs.

For example, a pharmaceutical OEM assembling products for a wellness brand may have access to their client, partner and supplier database. This is where manufacturers will have accountability for the personal data within their respective databases.

© 2019 Swivel Secure

Sensitive business data

Although it's not as tightly regulated as personal data, business data is highly sensitive, such as intellectual property, planning and production processes, and these are all at risk of cybercrime.

The position of Tier Two and Three manufacturers in the supply chain means they may not hold personal data, but they do have access to confidential business information like blueprints or intelligence. If intellectual property is stolen, it could have catastrophic consequences, in some instances an entire business can be lost due to commercial espionage.

Manufacturing is falling behind

The EEF's Cybersecurity for Manufacturing report found that 59% of manufacturers said they've been asked by a client to show or guarantee the robustness of their cybersecurity processes. Failure to comply with GDPR can lead to a fine up to 4% of a business' global turnover, or €20 million Euros. So, it's no surprise that businesses are looking to test the robustness of any third party who will have access to the data they safeguard – and even make it a contractual agreement.

A breach of business data could also be costly – losing confidential blueprints to theft or industrial espionage could have dramatic legal and fiscal implications for the Tier Two or Three manufacturer it was stolen from and affect the wider supply chain. But 37% of manufacturers said they couldn't make any assurances to their clients. And with the repercussions of non-compliance being so costly along with the risk of losing business data, clients and other manufacturers in the supply chain will be put off by a lack of cyber hygiene.

So how can manufacturers ensure they don't lose business because they're not cybersecurity savvy? Here are 7 of our top cybersecurity tips for manufacturers to follow to mitigate the risk of attack.

1. Train your employees

Human error has been found as a contributing factor in many cybersecurity breaches. AIG reports more than 80% of all cyber losses have a human element. A loss may be the result of accidental or malicious behaviour but can be caused by something as simple as clicking on a link.

In 2015, attackers gained access to a German steel mill through the plant's business network. A phishing email was sent to an employee who opened the malicious attachment. The hackers were then able to infiltrate a number of systems including the manufacturing execution system (MES) to control plant equipment and caused physical damage.

The first thing manufacturers should do to ensure good practice is to train all employees on basic cyber security. It's important for all users to understand that no matter their job title or responsibilities, they could be an entry point for attack, just by using a PC or laptop to access the network.Here are three key areas to train your team in:

• Educate employees on phishing scams

Phishing emails are becoming more advanced and can look harmless – often seeming to come from a trusted sender. Provide training on how to identify a malicious email, link or attachment and put a clear process in place for employees to follow if they think they have been sent a phishing email.

• Provide best practice for passwords

Make sure employees are aware they shouldn't write down, share or re-use passwords on other systems. Use a simple algorithm to always "salt" your passwords from entry point to entry point, so that a "contamination attack" (where a hacker grabs your password form entry point X and re-uses it on entry point Y) isn't possible.

• Make it a policy to only log in to the network from approved company devices and locations

Employees using personal laptops and phones or external internet connections to access the business network present another entry point for attackers. It's difficult for IT administrators to properly secure these external devices or connections so employees should be provided with company-approved devices that have been configured for working remotely.

© 2019 Swivel Secure

2. Use the appropriate level of security

In any instance where employees are using a device to remotely access the network, you should implement an appropriate level of security. An employee needing to access the enterprise resource planning (ERP) system from a coffee bar using their mobile device, or an office administrator who needs to send an internal memo, using Office 365 on a PC in head office, will require different levels of security for their tasks.

Risk-based authentication (RBA) utilises a set of rules and a points system to allocate the level of security required on a per user, per application basis. This can be based on a number of variables including: their physical location (GeoIP), the service being accessed, IP Address, last authentication, X509 Cert or device. This method of authentication is designed to be flexible and efficient for employees to use. It will help to increase the level of security without interfering with everyday work.

3. Ensure all applications are up-to-date

Another way manufacturers can improve their cybersecurity is to make sure any applications employees might require access to are kept updated. IT applications like Microsoft Word present another potential entry point for attackers. New versions are released regularly and often fix any weaknesses within the application that could be a security threat. This year alone, Microsoft released over 70 patches and Adobe, over 100 patches to their apps.

Although updating software is time consuming, and administrators often need to deal with aftermath from updating software such as memory leakage or software and driver compatibility issues, not doing so could potentially lead to a security breach.

Manufacturers need to make sure there is a process and the time set aside to update applications. This helps to remove one variable that could be a weak spot and see your system infiltrated by cyber criminals.

4. Use a jump host

Due to the connected nature of manufacturing supply chains, manufacturers need to include security points to prevent hackers gaining access to multiple systems. For example, PLCs (programmable logic controllers) which control hardware for manufacturing such as pick-and-place machines and other automated machines in manufacturing including computer numerical control (CNC) machines, can easily be hacked if they aren't protected on the network.

This can cause catastrophic consequences if any sabotage goes undetected for any significant amount of time – dependent on production. The PLC attacks are the jump from a virtual world attack to a real-world attack, as we saw in August 2017 when a petrochemical plant in Saudi Arabia was infiltrated by hackers with the intention of causing a physical explosion.

PLCs need to be protected from unauthorised access. A Jump Box or Jump Server can help protect them from external threats. This uses a computer on an insulated network which allows the PLC to be accessed by authorised personnel. The PLC and computer is linked externally when it needs updating but is protected at all other times – closing the connection to attackers.

The insulated network could also be secured with multi-factor authentication (MFA). In addition, if your PLCs also support RADIUS protocol, adding 2FA or MFA to the RADIUS authentication can further protect all the PLCs from cyberattacks.

© 2019 Swivel Secure

5. Apply single sign-on to access your separate networks

An infrastructure where hardware such as PLCs sit on insulated networks, and are separate to any external facing networks, will help to prevent hackers gaining access to the whole network. But manufacturers may regularly need to access systems seamlessly and without compromising security. Some systems might include:

- Customer Relationship Management tool (CRM),
- Enterprise Resource Planning (ERP),
- Product Lifecycle Management tool (PLM)
- Management Execution System (MES)

With so many tools and systems to keep separate, employees may require separate log-ins for each, meaning there's a multitude of usernames and passwords to remember. This can slow down or complicate working processes.

Although single sign-on (SSO) can provide greater efficiency, giving employees access to all platforms and systems (even if they are on different networks), it's imperative that risk-based authentication is utilised with SSO functionality, to ensure continued security.

6. Use multi-factor authentication

But it's not just enough to have a password for SSO. All the applications, systems and more on your network could also be secured with multi-factor authentication. This asks the user for a few pieces of evidence, like a password and a numerical code, before giving them access to the network.

Choose your MFA supplier wisely and be aware that although some two-factor authentication applications can be prone to credentials theft – they only update the code every 40-seconds, during which time a hacker can use the code to access the network.

Dedicated MFA platforms offer more secure authentication and are updated frequently to stay one-step ahead of cyber criminals such as delivering new security strings for each access request. However, there are a few elements of an MFA platform to consider so you achieve the maximum benefit, including:

• Efficiency – while SSO isn't enough on its own, some MFA platforms will allow for an SSO option and this is ideal for ensuring efficiency

• Flexibility – organisations are continually evolving, and the IT set-up needs to support the changing business. Your MFA platform should be able to integrate with hundreds of applications, so you're not restricted in the future

• Intelligence – with so many devices being used to access applications and employees travelling all over the world for work, it's important to be able to adapt your MFA platform based on any attributes you set. For example, you might configure the platform to recognise users based on a list of parameters like job title and give them access to the relevant platforms rather than the entire network.

© 2019 Swivel Secure

7. Aim for maximum adoption

Your cybersecurity features will only be effective if they're used in the right way. So manufacturers need to make it as simple as possible for employees to follow any security processes. If they are too complicated or interfere with everyday work, then getting employees to follow them will be difficult.

As well as providing a flexible MFA platform, streamlining processes with SSO options and offering training, you should help your employees understand why cybersecurity is critical for the manufacturing industry. Information about how attacks happened to other manufacturers will help your employees better understand their role in protecting the entire company.

It's not just one of these solutions that will help you protect your manufacturing business from a cyberattack. You should follow a combination of practices to make sure you can guarantee clients the robustness of your cybersecurity.

Different solutions will work for different companies and maximum adoption is key to make sure there are no weak spots in the network. So, it's important for you to find the solutions that suit your business and way of working.

FAQs

Manufacturing Cybersecurity

Swivel Secure have been supporting manufacturers with their authentication requirements for more than a decade. From steel production and electronic PCB assembly, to large scale ærospace and automotive manufacturers, Swivel Secure's AuthControl Sentry® is a pivotal part of their IT infrastructure, protecting their applications and data from unauthorised access.

© 2019 Swivel Secure

Can Swivel Secure provide authentication for Enterprise Resource Planning (ERP)?

Yes, Swivel Secure's AuthControl Sentry® can provide authentication for manufacturer's enterprise resource planning (ERP) software. Whether your organisation utilises SAP or Oracle, AuthControl Sentry can provide multi-factor authentication to prevent unauthorised access into your ERP system. With an extensive range of authentication factors from image authenticators using the patented PINsafe technology, or a simple one-time code (OTC) using a mobile app, deployment can be implemented ensuring maximum adoption throughout the business.

Can you still support us if we change our architecture?

AuthControl Sentry® is extremely versatile and can continue to provide multi-factor authentication both on-premise and cloud. Supporting SAML, RADIIUS, API and XML protocols means AuthControl Sentry® can integrate with most applications, providing your business with the flexibility it needs to grow and remain secure.

Can we use MFA to protect our Customer Relationship Management (CRM) database?

When your CRM is run separately from your ERP system, it can sometimes get overlooked. Utilising multi-factor authentication to protect your CRM is critical when you have a large sales team, accessing customer data using different devices from different locations.

Not only does AuthControl Sentry® protect your CRM from unauthorised access, it can deliver a risk-based authentication (RBA) solution, based on what form of authentication is deemed appropriate for any given user, or group of users. Using a set of rules, and a points system, a business is able to allocate the level of security required on a per user, per application basis. This can be based on several factors from the device being utilised to gain access, to the time and location of the last successful access.

Can Swivel Secure provide authentication for a Jump Host or Jump Server?

Yes, Swivel Secure recognise the need to utilise a jump server for manufacturer's to secure zone or manufacturing execution system (MES) and a demilitarized zone (DMZ). As the access to jump server requires close control, we strongly recommend using multi-factor authentication to ensure access is only permitted to the administrators entitled to manage it.

Using AuthControl Sentry® to secure your jump host allows you to define strict authentication requiring access. This can include multiple factors to allow authentication including tokens and tokenless factors including PINpad® (using PINsafe® patented technology), OneTouch PUSH option using the mobile app and biometrics such as fingerprints.

© 2019 Swivel Secure

Can we protect our regular applications such as Office 365?

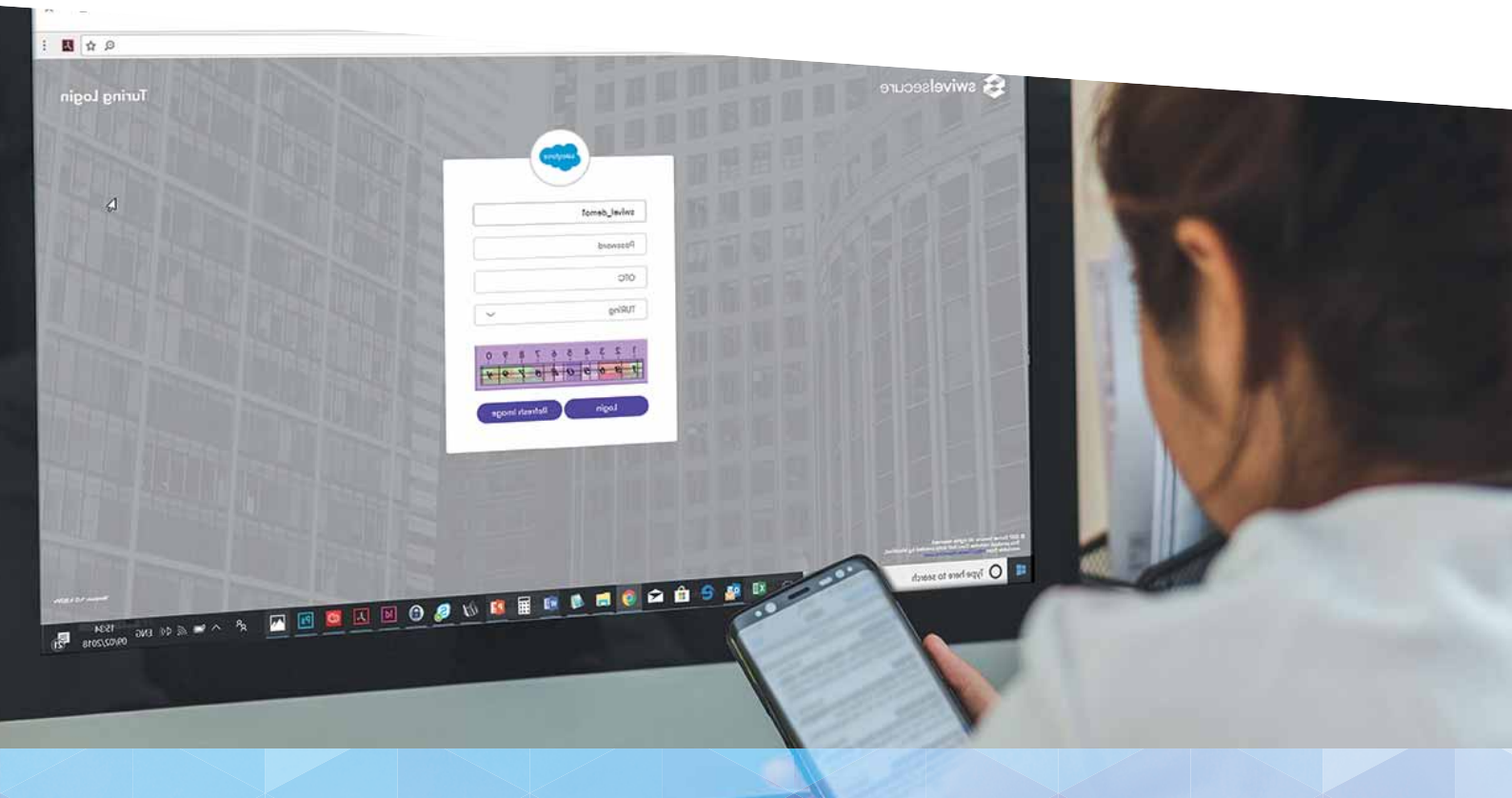
Yes, whether accessing your regular applications locally, through VPN, or Cloud, AuthControl Sentry® can protect all of your regular applications from unauthorised access including Office 365, Salesforce and SAP.

Saving costs and help-desk time, users can benefit from a self-service user portal where they can manage (change or reset) their own PIN, and provision the mobile app to use as an authenticator.

Does AuthControl Sentry provide authentication for PLM systems?

There are a range of product lifecycle management (PLM) systems available, some of which are open source and consist of a configurable authentication mechanism. In this instance, AuthControl Sentry® can usually be integrated into the PLM system to ensure there is no unauthorised access.

Both SAP and Oracle also provide PLM modules and these can be protected by AuthControl Sentry®, with a range of authentication methods. However, if you are using separate CRM, ERP and PLM systems, AuthControl Sentry® provides single sign-on (SSO) functionality, delivering increased efficiency, providing a secure and single source of access.



Protecting identities with intelligent authentication

USA & APAC Office
Swivel Secure, Inc.
1340 Reynolds Ave. #116-285
Irvine, CA 92614
E: **usa@swivelsecure.com**
T: **+1 949 480 3626** (Pacific Time)
Toll Free: **866.963.AUTH** (2884)

UK & Ireland
1200 Century Way
Thorpe Park
Leeds
LS15 8ZA
E: **hq@swivelsecure.com**
HQ T: **+44 (0)1134 860 123**
Support T: **+4 (0)1134 860 111**

EMEA Offices
Portugal
Estrada de Alfragide,
N67 Lote H, Piso 0 (Alfrapark)
2614-519 Amadora
Alfragide, Portugal
E: **portugal@swivelsecure.com**
T: **+351 215 851 487**

Spain
Calle Punto Mobi 4,
28805 Alcala de Henares,
Madrid, Spaind
E: **espana@swivelsecure.com**
T: **+34 911 571 103**

swivelsecure

www.swivelsecure.com