Healthcare:

Securing your organisation from online threats

swivelsecure

Contents

Introduction

Healthcare

Technological advancement has perhaps been most prevalent in Healthcare. From patient care to the daily jobs of healthcare professionals, the industry has been transformed by computerization.

Many processes have become more efficient, such as the retrieval of patient records, but the benefits new technology offers comes with its drawbacks. Healthcare has become a prime target for cybercriminals looking to exploit sensitive patient details or disrupt crucial work.

Find out more about how you can secure your organisation's network and protect against cybercrime in this brochure.

Article

9 reasons healthcare is a target for cyberattacks

Organisations are becoming increasingly susceptible to online attacks – threatening day-to-day work and compromising confidential patient data. Long, busy days mean healthcare staff don't have the time and resources to educate themselves about online risks. The potential disruption caused by a complete overhaul in online security is just too big for a lot of organisations to even consider.

Healthcare leaders are ready to increase spending on cybersecurity. But with new threats uncovered every day, it's difficult to know where an organisation would be better off investing their budget. High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks.

1. Private patient information is worth a lot of money to attackers

Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target. These organisations have a duty to protect their patients' personal records plus a legal responsibility to comply with GDPR guidelines.

Financial penalties – whether they be fines for not cooperating with GDPR or paying to retrieve their data from ransomware – are real and an alarming thought for a healthcare industry that's already struggling with financing daily work demands.

IT professionals are realising that the cost of securing their data with solutions like multi-factor authentication (MFA) is far less than the pay-out from ransomware or similar attacks. MFA is a solution that requires more than one piece of information to identify a user and then generates a one-time password on each login session. This makes it a lot harder for hackers to steal passwords and other information.

2. Medical devices are an easy entry point for attackers

There aren't many downsides to innovations in healthcare technology these days. Medical devices like x-rays, insulin pumps and defibrillators play a critical role in modern healthcare. But for those in charge of online security and patient data protection, these new devices open-up more entry points for attacks. Medical devices are designed for one purpose – like monitoring heart rates or dispensing drugs. They're not made with security in mind. Although the devices themselves may not store the patient data that attackers pursue, they can be used to launch an attack on a server that dœs hold valuable information. In a worst-case scenario, a medical device can be completely taken-over by hackers, preventing healthcare organisations from providing vital life-saving treatment to patients.

Hackers know that medical devices don't contain any patient data themselves. However, they see them as an easy target, lacking the security defenses found on other network devices like laptops and computers. Threats against medical devices can cause problems for healthcare organisations – giving hackers access to other network devices, or letting them install costly ransomware. Keeping network devices secure wherever possible, helps to limit the damage that could be caused by an attack on medical devices.

3. Staff need to access data remotely, opening-up more opportunities for attack

Collaborative working is key in the healthcare industry, with units working together to provide the best solution for every patient. Those who need to access information aren't always sitting at their desk – often working remotely from different devices.

Connecting to a network remotely from new devices is risky, as not all devices will be secure. Additionally, healthcare staff aren't often educated in cybersecurity best practices. It's crucial that compromised devices can't gain access to the network - just one hacked device can leave a whole organisation open to attacks.

One option for organisations that have staff working across devices is risk-based authentication (RBA). This solution makes risk analysis simpler by letting IT staff set up policies that determine the risk of a given device based on factors like the user, their location and more. Any unusual activity is then flagged to make sure that sensitive patient data is never exposed to unsafe devices.

4. Workers don't want to disrupt convenient working practices with the introduction of new technology

Healthcare staff are some of the busiest and most in-demand in the country. They work long hours and to tight deadlines – which means they simply don't have the time or resources to add online security processes to their workload. Medical professionals need slick working practices with minimal distractions.

Any cybersecurity measures placed on healthcare organisations need to consider the impact they may have on current working practices. IT staff should try to align security measures with existing software. There are plenty of authentication solutions available that work seamlessly with software like Office 365, meaning medical staff can perform their daily tasks without distraction.

Using Single Sign-On (SSO) solutions means authorised users can access multiple applications using just one single set of login information – keeping their working routines quick and simple, without compromising security. Frictionless solutions like SSO and RBA offer effective protection against online threats without disrupting the way people work.

5. Healthcare staff aren't educated in online risks

Medical professionals are trained to deal with a lot – but education in online threats is not in their schedule. Budget, resources and time constraints mean it's simply not possible for all healthcare staff to be fluent in cybersecurity best practice.

Cybersecurity solutions are complex, but their interface needs to be simple. Medical staff require a secure network that is quick and easy to access. And they need the peace of mind of knowing patient data is protected, so they can focus on their jobs. Solutions like MFA and SSO are becoming more popular as they simply use a secure one-time code – adding extra layers of security that don't require the user to know anything more than their own login credentials.

6. The number of devices used in hospitals makes it hard to stay on top of security

Modern healthcare organisations are responsible for massive amounts of patient data, plus an extensive network of connected medical devices. Larger organisations can deal with thousands of medical devices – all connected to their network, and each one acting as a potential threat for attackers.

Healthcare staff are often too busy to stay educated on the latest threats to devices, leaving IT specialists with the task of protecting an entire hardware network against attacks. If just one device becomes compromised, it opens the whole network up to data breaches and medical device hacks.

There is a need for healthcare professionals to be able to manage their own devices to an extent – freeing up IT specialists to deal with wider IT and security issues within the network. Some MFA solutions offer a self-service portal, which allows users to reset security PINs and more by themselves, helping to lighten the workload on the support desk.

7. Healthcare information needs to be open and shareable

Confidential patient data needs to be accessible to staff, both on-site and remotely, and on multiple devices. The typically urgent nature of the medical industry means staff need to be able to share information immediately – there's no time to pause and consider the security implications of the devices they're using.

The worry for IT staff is that the devices used to share information are not always protected. They can't always be there to assess the credentials of every device, especially in a time-critical environment. Users accessing data remotely will only need privileges for the tasks they'll need to perform. So, if they're just checking their emails, they won't need to have full admin account privileges. Precautions like this limit the chance of admin accounts becoming compromised.

Any solution that can save time and money by automatically regulating user permissions, without putting patient data at risk, is a must have for healthcare companies. MFA solutions prevent attacks from compromised credentials or unauthorised users to ensure only the right people can access sensitive data.

8. Smaller healthcare organisations are also at risk

All healthcare organisations are at risk from online threats. Large enterprises hold large amounts of data – representing the biggest bounty for attackers and placing them as common targets. But smaller enterprises have smaller security budgets. And less complex and up-to-date cybersecurity solutions mean smaller enterprises are often seen as an easy target, and as a backdoor-access opportunity to target larger enterprises.

Effective cybersecurity solutions have become a must for healthcare organisations of all sizes, as they're all in charge of sensitive patient data. Healthcare leaders are becoming more aware of the need to increase spending on cybersecurity – and there are plenty of solutions out there that are scalable to different business sizes. MFA solutions provide extra layers of security to your devices, using a combination of user passwords and one-time information that work for your company, and prevent attackers from stealing login information.

9. Outdated technology means the healthcare industry is unprepared for attacks

For all the incredible advances in medical technology in recent years, not every aspect of the healthcare industry has kept pace. Limited budgets and a hesitancy to learn new systems often mean that a lot of medical technology is becoming outdated. Hospitals using systems that still release system updates should keep all software equipped with the most recent version.

These usually contain bug fixes to keep systems fairly secure. But eventually, software will become end-of-life, and vendors will stop providing updates. Where it's not possible to upgrade to different, more secure software – or where medical staff simply don't want the hassle – it's possible to minimise the risk of cyberattacks by adding extra layers of security. If one system is compromised then an MFA solution can limit the lateral movement of an attacker through the network, as they won't be able to log-in to other protected systems.

Healthcare organisations have a responsibility to react to the latest online threats to keep their patient data secure. It's important to allocate a budget and invest in the right solution for your enterprise. Consider how your staff like to work and keep on top of new threats as they emerge – before your systems become outdated and you struggle to protect all your devices.

Infographic

Cybersecurity threats to the healthcare industry

Confidential patient data is being targeted at a huge cost to healthcare organisations. As online threats increase, hospitals need to increase their security budgets and IT specialists need to invest in the right security solutions for them and their staff.

Since the 2017 WannaCry attack...

200
NHS trusts fail latest cybersecurity standard

300,000
affected computers in

150
countries

£26 million+
set aside for the NHS to create a data security centre

The scale of cybersecurity

The estimated cost of cybercrime to the UK is **£27 billion** per year

of which around **33%** results from IP Theft from UK businesses

with up to **£1.8 billion** from the healthcare industry alone

What are some of the vulnerable access points?

Wireless connectivity & sensors increase potential exposure points, leaving doors open to cyber hacks

Critical medical equipment including **CT & MRI machines** remain vulnerable to cyber attacks

Cybersecurity & technology future predictions

Cybercrime damages will cost the world **$6 trillion** annually by 2021

Global spending on healthcare cybersecurity products will total **$65 billion** between 2017 - 2021

By 2022 there will be **6 billion** internet users

75% of the predicted world population

Every **40 seconds** a business falls victim to ransomware attacks

This is expected to become every **14 seconds** by 2019

Swivel Secure cybersecurity recommendations

MFA can be used to protect admin privileges, preventing unauthorised attacks

Use **RBA** to automate the process of assessing devices based on things like user / location

Self-service reduces the workload on support desk staff as users can redeploy the mobile app, reset pin etc

swivelsecure

www.swivelsecure.com

Article

How to secure patient data without overhauling your working practices

Healthcare organisations can store the data of thousands of patients. Confidential information like names, addresses, and personal medical information. And that private patient data is worth a lot of money to hackers. It's this wealthy online database, coupled with a network security that's often inadequate, that has made the healthcare industry the biggest targets for cyberattacks.

The challenge facing hospitals is that healthcare staff are simply too busy with their primary roles to focus on security measures and checks. They need work processes to be as seamless as possible to ensure they meet tight schedules. So overhauling the working routines that healthcare staff are familiar with in favour of a new security process is impractical, and could cause more harm than good in a time-critical industry.

A busy environment, plus the need for organisations to be HIPAA and GDPR compliant, make the task of securing patient data complicated. Here are four ways choosing the right patient data protection solution can work for your healthcare organisation.

Become HIPAA and GDPR compliant with secure software

Any organisation that deals with medical records in the US has a duty to become HIPAA (Healthcare Insurance Portability and Accountability Act) compliant – protecting confidential patient data from being shared with, or accessed by, unauthorised users.

HIPAA compliance requires US healthcare organisations to put suitable 'technical safeguards' in place to make sure their data is protected and provides a solid benchmark for any organisation in the healthcare industry worldwide. Companies that fail to comply risk finding themselves with a substantial fine.

General Data Protection Regulation (GDPR) also asks for strict data security measures to be put in place. The regulation says that any company that holds Personally Identifiable Information (PII) for EU citizens must provide reasonable protection for the data – and this significantly affects healthcare organisations, who have thousands of patients' data on record.

Data-protection regulations provide a different challenge to healthcare organisations than those of cyberattacks – but the financial implications can be just as damaging. Hospitals need to invest in secure solutions to protect their information, helping to save on costs long-term for failing to meet government standards.

IT staff have to keep their organisation's data secure. So, any solution that is simple to integrate and get staff up-to-speed with will save time and effort.

Solutions like Multi-Factor Authentication (MFA) integrate with a range of devices, to complement the way an organisation likes to work. This is easier to roll out to hospital staff as it does not steer too far from their existing working patterns. MFA asks users for multiple login credentials, like a password plus a one-time code (OTC), to stop unauthorised users from accessing patient data.

Swivel Secure's AuthControl Sentry® keeps patient data exclusive to staff using Risk-Based Authentication (RBA). The solution assesses the risk of each login attempt, based on factors like IP address, location, and the device being used to access the network. If a user's activity is deemed unusual, they'll be asked for a higher level of authentication for added security.

Choose a solution that integrates with your existing software

Time is invaluable to healthcare staff. Packed schedules mean they can't afford to add new processes into their daily workflow. They need to use software and medical devices fluently to work to tight deadlines. So, it's important to keep tasks consistent while improving network security, and IT staff should invest in a solution that causes as little disruption as possible.

Solutions like Swivel Secure's AuthControl Sentry® software integrate with systems including Office 365 – to better protect patient data, without drastically changing the way staff already work. This makes the process easier for the help desk, who won't have to train staff on completely new systems, but just need to roll out an extra step or two to tighten up network security.

Outdated legacy systems are often incompatible with new authentication solutions or can't update to include authentication support. But Swivel Secure can tie many of these existing systems together with secure MFA, without introducing brand new software for staff to learn. This smooth integration makes it easier for entire organisations to get used to new healthcare security measures, working within systems they're already familiar with.

MFA only requires an extra few seconds for users to log-in to the network, and Swivel Secure's Single Sign-On (SSO) solution lets users securely access multiple systems using only a single log-in. Making it a hassle-free solution for healthcare organisations.

Use a solution that integrates seamlessly with all devices

Healthcare workers rarely sit at a desk. They're constantly on the move, working from any nearby or remote device they can access – including mobile devices. Medical records often need to be shared or accessed instantly, but healthcare organisations cannot compromise on security.

Patient data-protection needs to work consistently across all devices and users. Installing secure MFA across your network allows users to access data remotely in a way that's convenient for them, without risking data hacks. Hospital staff can verify their login credentials using a mobile app, SMS code, hard token or another MFA verification method – to access patient data on any device needed.

Swivel Secure's AuthControl Sentry® uses RBA to automatically manage third-party access. Healthcare staff need to use multiple devices daily, which can cause third-party access risks. But by limiting access by device type, time of day, IP address and more, hospitals can prevent unauthorised users from accessing the network. Automating this process also takes one extra worry away from the IT desk, and frees them up to tackle other network security issues.

Invest in software that works for your company

Any healthcare organisation investing in data security needs to consider the way their staff work and how the company operates. Introducing data-protection solutions that clash with how an organisation runs can be costly and inefficient.

Hospitals may wish to invest in an MFA hardware token solution – equipping staff with a key fob token that provides a one-time log-in code to securely access a patient portal. Hardware tokens are single, small fobs that don't require additional devices like mobile phones to receive a log-in code. But they're a more expensive option for large companies, with the risk of constantly replacing lost key fobs.

Token-less MFA solutions include SMS or mobile-app options, and simply provide users with a one-time code when they need to log-in to a patient portal. This is quick and easy for staff that carry a mobile at work. Tools like Swivel Secure's PINsafe offer a cost-effective solution to large organisations – combining the use of a registered PIN with 10-digit security strings that are sent by SMS, Mobile app, or web, and avoids the hassle of IT staff replacing lost tokens.

Swivel Secure's AuthControl Sentry® solution offers both token and token-less options – and can help with efficiency too, as it is intuitive to use. AuthControl Sentry® lightens the workload on the IT desk by providing hospital staff with the ability to change or reset their PIN and re-provision their own mobile app account (it will have to have been originally provisioned by an administrator). Hardware token users can also re-sync their token without having to call help.

FAQs

Healthcare Cybersecurity

At Swivel Secure we are proud to be able to offer a cost-effective multi-factor authentication (MFA) platform for the healthcare industry. Read answers to some frequently asked questions (FAQs), often asked by our healthcare users. AuthControl Sentry®, the multi-factor authentication platform from Swivel Secure protects a wide range of applications including Office 365.

Can Swivel Secure provide authentication for healthcare professionals accessing patient records?

Yes, Swivel Secure's AuthControl Sentry® can provide an additional level of authentication for accessing patient records. Multi-factor authentication is a security system that requires more than one method of authentication. Independent categories of credentials to verify the user's identity are used for establishing authentication, including mobile app, SMS, email, and token based authenticators. AuthControl Sentry® is at the core of the platform and protects your networks, systems, applications, and data.

Can the Swivel Secure platform AuthControl Sentry® protect Office 365?

AuthControl Sentry®, the multi-factor authentication platform from Swivel Secure protects a wide range of applications including Office 365. The platform provides two-factor authentication, risk-based authentication, and single sign-on functionality. AuthControl Sentry® can integrate with both Microsoft ADFS 3 and ADFS 4.

How would authentication for staff accessing patient records be managed?

Using AuthControl Sentry® to manage access to data requires minimal operational overhead. The self-service user portal with integration into active directory and automated user provisioning, can save overheads and maintenance costs by reducing the burden on the help-desk. With the self-service user portal doctors and physicians can change or reset their pin, re-sync hardware tokens and download the mobile app to use as an authentication method.

Can Swivel Secure provide authentication for patients to access their records?

AuthControl Sentry® has the flexibility to protect a wide range of applications and data access points. Ideal for utilisation with a patient portal, AuthControl Sentry® can securely protect access to patient data with a range of authentication factors. The ease of use and flexibility of the platform enables patients to use a range of devices to authenticate access including mobile phones. Both short messaging service (SMS) and the mobile app can be used, offering optional authentication methods including a OneTouch PUSH authentication, allowing users to simply accept or reject the authentication.

Can AuthControl Sentry® help to protect data from third party access?

Hospitals regularly have a requirement for third party organisations and individuals to access data, ranging from technical engineers to auditors. This can be hard to manage and control, but with AuthControl Sentry® third parties can be managed using risk-based authentication ensuring secure access based on set criteria such as a known IP address.

Protecting identities with intelligent authentication

USA & APAC Office
Swivel Secure, Inc.
1001 4th Ave #3200
Seattle
WA 98154
E: **usa@swivelsecure.com**
T: **+1 949 480 3626** (Pacific Time)
Toll Free: **866.963.AUTH** (2884)

UK & Ireland (North)
Equinox 1, Audby Lane
Wetherby, Leeds
LS22 7RD
E: **hq@swivelsecure.com**
HQ T: **+44 (0)1134 860 123**
Support T: **+4 (0)1134 860 111**

UK & Ireland (South)
Pinewood
Chineham Business Park
Chineham, Basingstoke
RG24 8AL
E: **hq@swivelsecure.com**
HQ T: **+44 (0)1134 860 123**
Support T: **+4 (0)1134 860 111**

EMEA Offices

Portugal
Estrada de Alfragide
67 Alfrapark - Lote H
Piso 0
2614-519
Amadora
E: **portugal@swivelsecure.com**
T: **+351 215 851 487**

Spain
Av. Juan Carlos I
13 - 2a planta (Torre Garena)
Alcalá de Henares
28806 Madrid
E: **espana@swivelsecure.com**
T: **+34 911 571 103**

swivelsecure

www.swivelsecure.com