avanade

Do what matters

Securing healthcare data in a hyrbid cloud environment

A guide to help protect personal health information and build resilience against cyber attacks.

Protecting patient data in a hybrid cloud environment

Cloud computing has offered a fast path for healthcare organizations to advance virtual care services such as telehealth and remote patient monitoring. In fact, 88% of healthcare organizations have accelerated spending on cloud migration.

The top reasons for the switch to a cloud-based infrastructure include remote working, cost savings and improved information technology agility. This accelerated switch has meant a growing amount of healthcare data is stored in a hybrid cloud environment. With this shift, healthcare organizations face the increased challenge of protecting vast amounts of data, on premise and in the cloud, securing access, as well as securing access to this information from multiple devices and varied sites of care.

How is your healthcare data accessed and secured?

Cyberattacks are increasing the need for healthcare organizations to rethink how data is accessed and secured.

These include poor handling of the digitization of patient records and movement of them to cloud services as well as the use of legacy tools that are too old to keep up with modern cybersecurity needs.

For many organizations, resetting on-premises security practices and processes to work in a hybrid cloud environment require adoption of a continuous security focused path forward.

Why cyberattacks may only increase

Personal Health Information (PHI) can sell up to 10 times more than credit card numbers on the dark web. If holding data hostage continues to prove financially lucrative, healthcare organizations will continue to be the targets of ransomware attacks.

85% of IT professionals surveyed at healthcare organization said that cyber risk has increased over the past 12 months.

A healthcare data breach costs healthcare organizations on average $7.13 million, up 10% from previous years.

It’s **more** than the cloud

It’s not just the cloud that’s driving fundamental change in how healthcare organizations manage and protect data and patient information.

Other key change agents include:

- The merging of digital and physical services has created an omnichannel ecosystem. Managing and protecting the growing number of multiple disparate applications and devices by facility and department can be challenging.
- Medical devices like x-rays, insulin pumps and defibrillators play a critical role in modern healthcare. But for those in charge of connected devices, these new devices open potential entry points for attacks.

A large hospital could be home to as many as 85,000 connected devices, resulting in a need to rethink existing security practices.

Confidential patient data needs to be easily accessible to staff, both on-site and remotely. 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.

Four accelerators to help protect healthcare data in a hybrid cloud environment

In this guide, you’ll find four accelerators to help create an achievable end goal, build zero trust principles, enhance threat protection and enable care teams to adopt a Zero Trust mindset.

1 Gather a baseline view

Assess current and future risks and define an achievable end state in a hybrid cloud environment.

2 Build zero trust principles

Improve the protection of your critical data assets by enabling Zero Trust through modern identity solutions.

3 Enhance threat protection

Rapidly close gaps as well as nurture an adaptive approach to enhance threat protection.

4 Secure care team collaboration

Promote solutions that mean distributed teams can connect and collaborate securely and efficiently.

Faster growth, lower cost, better trust

Organizations that embed security and privacy into the design of digital transformations to cloud, for example, grow faster at a lower cost with better trust.

1. **Gather** a baseline view

Identify priorities for improvement aligned with security and organizational goals

It's important to gather a baseline view so you have an accurate picture of your security landscape and understand what your key risks are and what areas you need to focus on

Align security to business goals

Organizations should identify priorities for improvement aligned with organizational and security goals. These can be broad, looking at the entire organization, or focused where needed — for example, on third-party risk or regulatory requirements.

Design a governance framework

Despite the huge variety of regional regulation, healthcare organizations must develop a baseline standard way of doing business, which should account for all the things you have to do from a compliance and risk standpoint. Having a governance framework in place, knowing where the risk lies, gives organizations a roadmap for what it should be doing to continually manage and improve things.

Create awareness and training

Create security awareness and training to enable your employees to become security advocates. Evaluate changes needed to make ongoing security awareness training current with a hybrid cloud workplace. Encourage the Board or senior executives to get behind and sponsor awareness campaigns across the organization.

Assess skilled resources

It's important to understand available skills and capabilities. If your healthcare organization does not have strong cloud skills, for example, then partner with someone who does. It will help get the job done right the first time, saving time and money.

How we're helping clients secure data and network access

NHSmail: The silent digital revolution

Clinical teams change the way they work; patient journey improves and cost efficiencies are unlocked

Challenge

The United Kingdom's population has increasingly complex health needs, and a multi-disciplinary approach is crucial when treating acute, elderly or multi-chronic patients.

Goals for the NHSmail were to bring different types of care professionals onto the system, connect them effectively, safely transition a user base of over a million and grow that to the current 1.4 million accounts.

Solution

The transition from a legacy NHSmail service to a new platform was designed, built, tested and delivered by Accenture and Avanade – a joint venture between Accenture and Microsoft.

Ongoing engagement services include application development and management, service desk outsourcing, infrastructure and technology consulting.

Results

Cyberattack protection

Preventing over 1 billion malicious emails every month.

Secure collaboration

Digital collaboration services enabled new healthcare practices and collaboration methods between health and social care organizations across England and Scotland.

Enhanced access

Professionals in 13,000 organizations have access to scalable and secure collaboration.

2. **Build** on zero trust principles

Move past traditional perimeter-based security to address modern hybrid healthcare environments

A Zero trust model can help healthcare organizations provision access in a more effective manner by focusing on data, workloads and identity

Bolster proactive security

Protect modern digital environments with Zero Trust principles designed to help organizations take a more proactive stance to clearly define goals, outcomes, and architectures for heighten security.

Identify risk areas

Identify and remediate areas of heightened risks associated with personal and shared home devices and peripherals – such as weak passwords, poorly secured home Wi-Fi routers and a lack of patching for remote systems.

Monitor and quickly react to risky behavior

Enforce conditional access automatically, limiting exposure at the identity level. Support this process by augmenting firewalls and other traditional security methods with modern identify and access management and authentication solutions using an "assume breach" model.

Consider how you can scale

Identity solutions to support secure access for third parties – patients, partners and Internet-connected devices including medical devices and bots. Review your privileged access management to secure, control, manage and monitor access to critical assets.

Rooted in the principle of "never trust, always verify," Zero Trust is designed to protect modern digital environments, embrace the mobile workforce and protect people, devices, apps and data wherever located.

How we're helping clients deploy zero trust strategies

A health insurance and healthcare group enhance security and threat protection

Managed digital identities and provided threat protection with Microsoft Azure Sentinel and Microsoft Windows Desktop

Challenge

The organization's platform was maturing and required a better toolset to address growth. The client also wanted to address the security and operational needs of the program.

Solution

This was a greenfield Microsoft Azure migration. Avanade's solution was provided in two releases and included building a Microsoft Azure Sentinel on the existing Microsoft Azure Security Center.

We designed and implemented a Microsoft Azure environment for protected workloads, and we also manage security services 24x7x365 using Microsoft Azure Sentinel for:

- Digital identity
- Application security
- Threat protection
- Security capacity services

Results

Digital identity

Implemented identity lifecycle management, self-service password reset, one identity active role manager and user management service desk

Threat protection

Implemented Microsoft Defender Endpoint, Microsoft Cloud App Security, Microsoft Defender Identity, Microsoft Azure Sentinel Integration, threat intelligence and vulnerability management

Rapid deployment

Adherence to strict client deadline for the first release managing a complete greenfield project

3. **Enhance** threat protection

Create next level detection and monitoring

As data becomes increasingly digitized, it is essential that healthcare organizations use the latest practices and technology tools to protectively detect risks

Use advanced tools to better detect risks

Build an evergreen security ecosystem using the most advanced tools so you can rapidly close gaps and enable new ways to securely communicate and efficiently work in a hybrid ecosystem.

- Azure Active Directory Identify Protection to better detect risks specific to your identity infrastructure.
- Microsoft 365 Advanced Threat Protection to quickly understand and respond to threats to your email and data.
- Azure Sentinel to provide better visibility and traceability over attack vectors, a path which an attacker or hacker can gain access.

Fine tune your incident response

Consider how a combination of managed security services and automation can fine tune your incident response (IR) and penetration testing.

Deliver the highest added value

Focus on quick wins for highest added value. Each win adds incremental value to reduce risk and improving the security posture of your digital estate. Share tangible outcomes with your executive leadership but balance immediate priorities with your future strategy requirements.

How we’re helping clients secure information at home and work

Remote information protection and access to an in-flight project with Microsoft Azure

Challenge
A regional hospital wanted to provide secure access to hospital data rapidly. However, it did not have the in-house capacity to respond to this challenge alone.

Due to the pandemic, hospital leaders wanted to allow doctors, nurses and non-clinical employees to work from home whenever possible.

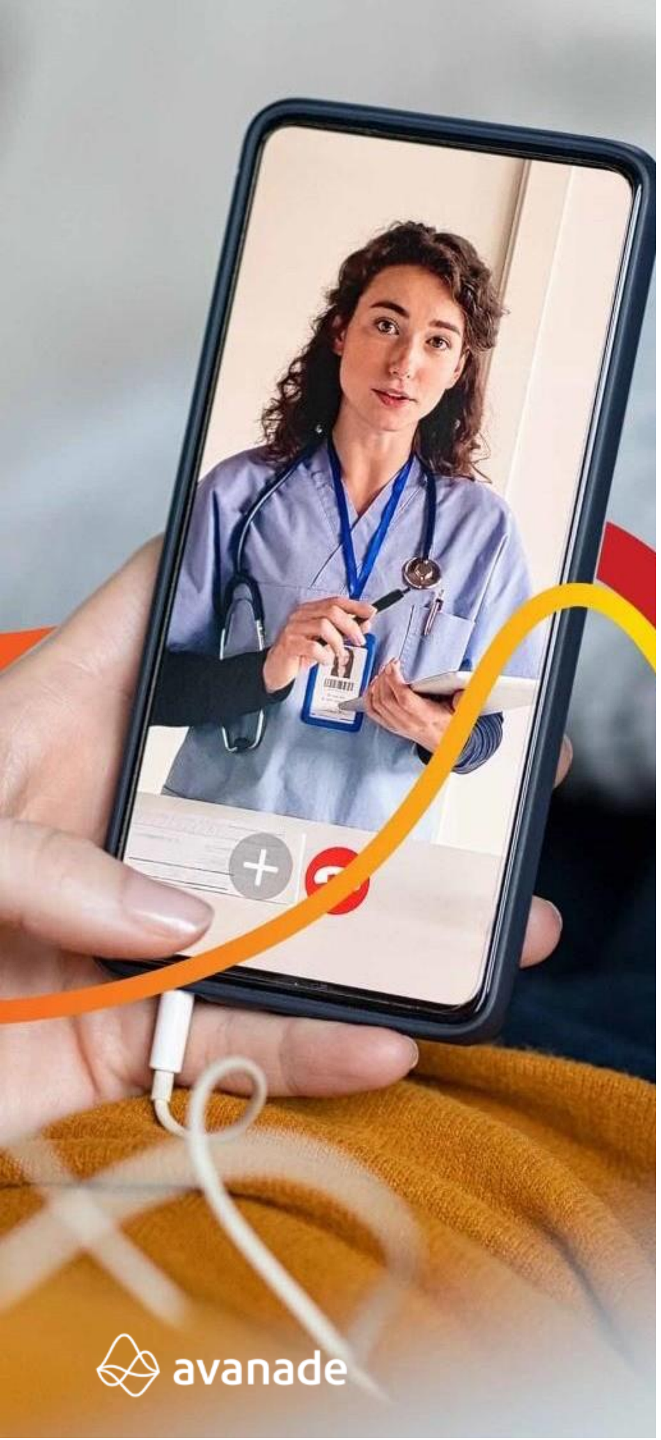
Solution
The Avanade team implemented a remote working solution that also prioritizes data protection and cyber defense. The solution was a Windows Virtual Desktop running on Microsoft Azure.

The security team designed and implemented secure remote access using cloud services. In addition, we helped clinicians and staff shift away from working on personal devices to Microsoft Azure, which enabled a rich performance anywhere and any time.

Results
Rapid deployment
Critical hospital resources went live within a week of the government ‘lockdown’

Cyber defense
Enhanced data protection and cyber defense with Microsoft’s cloud security services

Rapid adoption
Minimal training required by using Microsoft 365 productivity and collaboration tools through familiar desktop for users.



4. **Secure** care team collaboration

Extend data protection to enable care team collaboration

More than most other industries, healthcare requires constant collaboration and communications between providers so it is important healthcare organizations ensure data is both easy for care teams to access and difficult to breach

Establish guidelines

Establish clear guidelines on how to share information securely based on data classification, audience and content type. Adopt and measure collaboration with the large-scale deployment and use of collaboration tools and by providing targeted, prescriptive guidance on how to be safe and secure when working remotely.

Enable secure remote and in-person collaboration

Be nimble and innovative with the latest technologies. Clearly communicate which officially approved software and tools may be used for remote working—including those for file sharing, video conferencing, virtual whiteboard collaboration and chatting.

Anticipate increase in collaboration tools

Anticipate the increase in volume and load from the use of collaboration tools by employees working remotely, while also improving usability and productivity. Encourage large-scale virtual sessions using interactive broadcast and web conference platforms to support the shift from physical to virtual care sessions, training and education.

How we’re helping clients secure collaboration

Leading provider of medical devices secures collaboration and information

Implementation of Microsoft 365 with Azure Information Protection to classify each document and protect information

Challenge

A medical and pharmaceutical device company needed to help colleagues around the world collaborate on the technology that will keep them healthy tomorrow. Microsoft 365 was the answer—but migrating 34,000 employees in more than 60 countries was a challenge. Different countries have different requirements and demands, that needed to be addressed before moving data into the cloud.

Solution

Avanade deployed the collaboration solution and the approach. This included a series of workshops with Avanade and the Microsoft FastTrack Team to scope, educate and allow multiple people to work together on the same document and comply with regulations.

Using Azure Information Protection to help fulfill the legal requirements of the various global regions was key to getting the company’s team on board with the Microsoft 365 implementation.

Results

Rapid deployment
Critical hospital resources went live within a week of the government ‘lockdown’

Cyber defense
Enhanced data protection and cyber defense with Microsoft’s cloud security services

Rapid adoption
Minimal training required by using Microsoft 365 productivity and collaboration tools through familiar desktop for users.

We’re here to help you secure and protect data and patient information

Microsoft 365 Security Assessment

What is it?

A comprehensive Microsoft 365 assessment covering industry standards, deep insights, reporting and remediation to help you address the security priorities required to sustain and scale a secure hybrid environment.

Outcomes

Address identified gaps to improve your security posture using existing Microsoft capabilities

- Protect against advanced threats and use
- Microsoft Intelligence security services
- Provide additional security and visibility for recently deployed services and infrastructure
- Improve compliance with advanced security controls
- Improve user experience and productivity
- Solve immediate hybrid working challenges while building towards longer-term business transformation

Time

- Three-week assessment

Activities

- Run three healthcare security domain workshops
- Process findings, produce recommendations and develop an action plan report and implementation roadmap
- Present executive report to senior client stakeholders and agree on next steps

Deliverables

- Security assessment report covering an extended set of domains
- Client-focused dashboard with additional analytics
- Benchmark against standards
- Detailed prioritization and remediation plan

Unparalleled **health and life sciences expertise** in securing the **Microsoft platform**

Avanade Health has a global practice of over 1,000 technical, functional and organizational change professionals, health strategists and consultants, serving health providers, payors life sciences and medical device clients.

Our security approach is shaped around business and IT priorities and based on the latest thinking about cyber-compliant and cyber-resilient digital and cloud solutions and business applications on the Microsoft platform.

We bring global scale and expertise to a broad healthcare market

The Avanade/Accenture partnership serves health providers, health payors, life sciences and medical device organizations. Through the work we do, we strive to make a positive impact for providers, clinicians, payors, biotech companies and their customers across 20 countries worldwide.

We're recognized for our Microsoft security and healthcare expertise

- 18 Microsoft Gold Competencies including gold for Microsoft Security Excellence Award winner for Zero Trust Champion
- Microsoft 2022 Global Alliance SI Partner of the Year – for the 17th time
- Member of the Microsoft Intelligent Security Association (MISA)
- Microsoft 2020 Global Healthcare Partner of the Year
- #1 globally in Teams and Office 365 deployment

We partner with clients worldwide

- 4,000+ clients since 2000
- 46% of Global 500 companies
- 34% of Fortune 500 companies
- 90% of Fortune 500 life sciences companies
- All top 10 global pharmaceutical companies
- Avanade/Accenture services 41 of the top 100 hospitals (U.S. Thomson Reuters)
- 21 out of 25 largest U.S. Payers

Reimagine data and AI

Partner with Avanade to help you reimagine your digital health journey with data and AI

Contact us today

North America

Seattle
Phone +1 206 239 5600
America@avanade.com

South America

Sao Paulo
AvanadeBrasil@avanade.com

Asia-Pacific

Australia
Phone +61 2 9005 5900
AsiaPac@avanade.com

Europe

London
Phone +44 0 20 7025 1000
Europe@avanade.com

Avanade is the leading provider of innovative digital, cloud and advisory services, industry solutions and design-led experiences across the Microsoft ecosystem. Every day, our 60,000 professionals in 26 countries make a genuine human impact for our clients, their employees and their customers. Avanade was founded in 2000 by Accenture LLP and Microsoft Corporation. Learn more at www.avanade.com