

eBook

THALES
Building a future we can all trust

Protecting healthcare and life-sciences data from a cyber-attack pandemic

cpl.thalesgroup.com



Digitalization enable expansion of patient-centric care and healthcare R&D

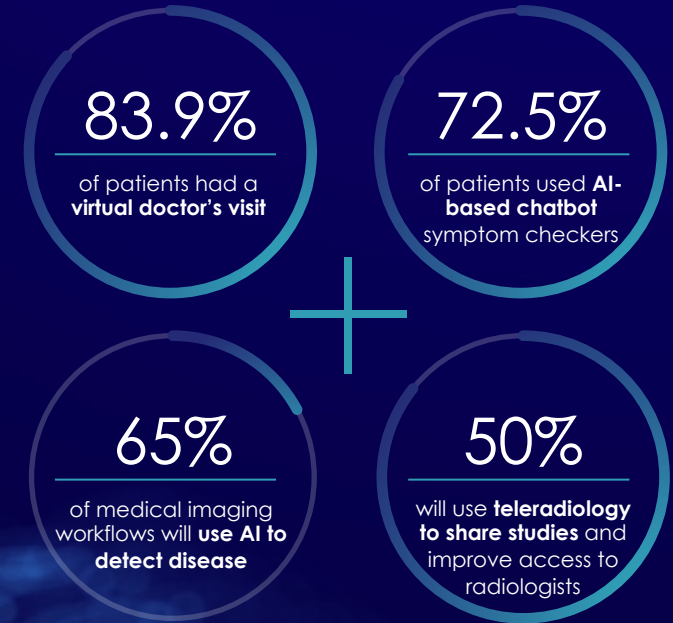
The healthcare and life sciences industries have been eagerly adopting new transformative technologies. Once slow to adopt, healthcare-related industries have, even before the pandemic, been rapidly embracing digitalization to enable patient-centric care that is more effective for patients and safer for patients, healthcare professionals and researchers.

The Covid-19 pandemic put this trend on overdrive, driving the adoption of connected health technologies that make a wide range of virtual care services possible.

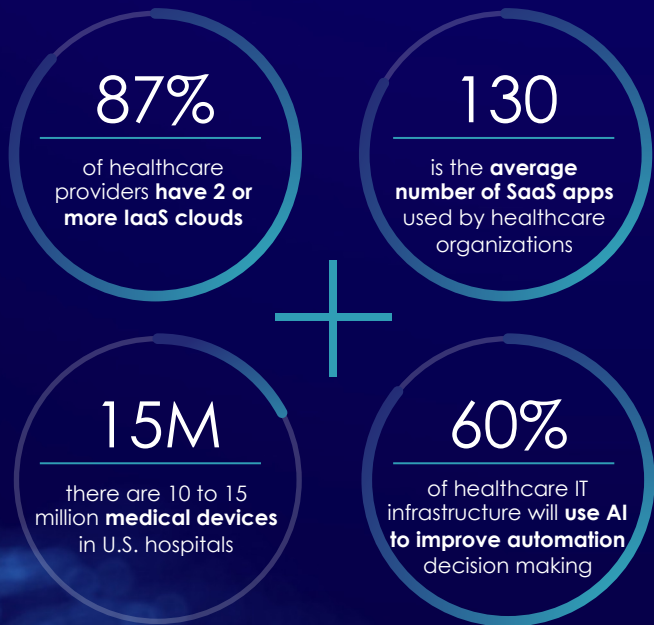
For example, IDC found 83.9% of 1,500 US survey respondents, who had a care visit during the initial pandemic wave, had a virtual visit for the first time. And 72.5% used Artificial Intelligence (AI)-based chatbot symptom checkers.¹

Looking to the future, IDC predicts that by 2026, “65% of medical imaging workflows will use AI to detect underlying disease and guide clinical intervention, while 50% will use teleradiology to share studies and improve access to radiologists.”¹

¹: IDC, Worldwide Health Industry 2021 Predictions



Driving adoption of a digital infrastructure



The healthcare and life science industries embrace of digitalization has been all encompassing. According to the 2023 Thales Data Threat Report – Healthcare and Life-Sciences edition, 87% of healthcare organizations have two or more cloud infrastructure providers (IaaS) and on average they use 130 software as a service platforms (SaaS).²

At the other end of the spectrum, the proliferation of connected medical devices and the internet of medical things (IoMT) have dramatically accelerated. According to IDC, today there are 10 to 15 million medical devices in U.S. hospitals with an impressive average of 10 to 15 connected medical devices per patient bed.¹

When combined, the ability to collect data in real time together with the massive processing power of the cloud provide the opportunity for dramatically improved decision making. IDC predicts that by 2024, "the proliferation of data will result in 60% of healthcare organizations' IT infrastructure being built on a data platform that will use AI to improve process automation and decision making."¹

1: IDC, Worldwide Health Industry 2021 Predictions

2: 2023 Thales Data Threat Report Healthcare and Life-Sciences edition

But increasing complexity and the chances of a cyber attack

While the digitalization of the healthcare and life sciences industry has led to better patient care, it has also made these industries potentially more vulnerable to attacks by cybercriminals. The main cause of vulnerabilities is complexity.

The sheer number of new platforms and technologies being adopted dramatically expands the attack surface, and creates challenges for the protection of different environments. For example, 60% of healthcare and life-sciences organizations reported having five or more key management solutions, and 55% of organizations think that securing data in cloud is more complex than on-premises.²

The end result is that more sensitive data could be at risk in more platforms. 68% of healthcare and life-sciences organizations reported that more than 40% of their data in cloud is sensitive. However, on average, only 45% of sensitive data in cloud is encrypted. That includes data regulated by the multiple privacy, security and resilience legislations that healthcare and life-sciences organizations need to comply with.²



Stricter cybersecurity mandates and legislation add urgency

The growth of cyber incidents has led to unprecedented executive and legislative action:



White House Cybersecurity
Executive Order



European Union
Cybersecurity Act

The convergence of existing privacy, sovereignty, and data protection regulations, such as HIPAA, GDPR, CCPA, and global standards such as ISO 27799:2016 on health informatics, raise the bar for healthcare and life sciences organizations, obligating the protection of sensitive personal data and levying substantial fines for not doing so.

The Executive Order to Improve the Nation's Cybersecurity and protect federal government networks and the nation's infrastructure was signed by President Biden in 2021. The order helps move organizations to secure cloud services and a zero-trust architecture and mandates deployment of multi-factor authentication and encryption.

The European Union's Cybersecurity Act passed in 2019 gives ENISA, the EU Agency for Network and Information Security, a permanent mandate. It also establishes a European cyber security certification framework for information and communications technology products and services. In particular, it calls for up-to-date software and hardware with mechanisms for secure updates leveraging code signing.

How Thales can help

Thales enables healthcare and life-sciences organizations to accelerate digital transformation by reducing risk, complexity, and cost.

Scale security across
enterprise hybrid IT



Automate and streamline data and
identity protection with **scalable** solutions
for multiple use cases

Accelerate digital
transformation



Adopt innovations such as **cloud, big**
data, AI, and IoMT faster with a
framework for a zero-trust world

Reduce risk and complexity



Simplify privacy compliance with
centralized data governance and
de-identified sensitive data

Scale security across enterprise Hybrid IT

Automate and streamline data and identity protection with scalable solutions for multiple use cases

Centralize key management for third-party security solutions across cloud, hybrid and on-premises environments

Minimize the threat of data breach by de-identifying all sensitive data in all new environments and legacy platforms, including partners and suppliers

Secure access to health records with MFA for all IaaS, PaaS, SaaS, and on-premises platforms.



SaaS, PaaS, IaaS services



On-premises legacy systems



File repositories and databases



External party collaboration



Remote medical devices



Challenge

- **AmerisourceBergen is a Fortune 10 healthcare enterprise** focused on the development and delivery of drugs and healthcare products. The company needed a solution that to safeguard privacy and protect sensitive customer health care data.
- The company required a fully automated, enterprise-grade solution that could enforce security policies on a wide variety of cloud-based and on-premises platforms. And desired a solution that would not decrease performance or availability of IT systems.



Solution

- **CipherTrust Data Security Platform** was implemented to centralize the key management of multiple databases as well as cloud and on-premises applications.
- **Simplified data protection** by centrally managing encryption keys and configuring security policies with granular access controls.
- Protected sensitive encryption keys in **FIPS 140-2 Level 3** tamper-proof HSMs.



Results

- **Improved HIPAA compliance** posture and helped maintain ISO 27001 and ISO 9001
- **Improved resiliency** of the entire hybrid IT infrastructure with high availability and optimized performance.
- **Seamless implementation** at scale of a complex solution touching many environments.
- **Supported the company's assurance** to clients that it is securely and efficiently protecting their data, and delivering on the promise of being a 'trusted data company.'

AmerisourceBergen

AmerisourceBergen ensures customer trust in the highly-regulated healthcare industry

HIPAA compliance and protection of PHI in
cloud and on-premises systems

Protection of sensitive data across hundreds of pharmacies in North America

Protection of sensitive data across legacy systems and new platforms



Challenge

- A **major pharmacy chain** had to protect sensitive data flowing between hundreds of locations and its headquarters.
- Data included patient records, financial information and intellectual property, each falling under different compliance requirements.
- Constant release of new IT capabilities required that the solution be extremely flexible and scalable.



Solution

- **CipherTrust Transparent Encryption** with **centralized key management** were deployed to protect sensitive data at rest multiple locations.
- Granular controls allowed the precise definition of which users are permitted access to which assets in the network.
- Enabled the seamless protection of a dynamic infrastructure with legacy systems and constantly changing new platforms.



Results

- **Achieved comprehensive data security coverage** across multiple locations and systems.
- **Enabled continued compliance** with multiple healthcare, financial, and other regulations.
- **Had no noticeable performance impact** on the systems achieving low financial and operational overhead.
- **Ensured future scalability and growth** by enabling easy addition of security to new platforms and data stores.

Accelerate digital transformation

Adopt innovations such as digital signatures, multi-cloud environments, Internet of Medical Things (IoMT), AI, and big data **faster with a framework for a zero-trust world**

Secure digital identities, applications, IoMT devices and cryptographic keys with a certified root of trust

Protect data in multi-cloud environments with BYOK, HYOK, BYOE, centralized key management

Adopt a zero-trust posture for all environments with MFA, intelligent SSO, and centralized access control



Digital records and signatures



Multi-cloud



Internet of Medical Things (IoMT)



Artificial Intelligence



Big data

Protection of innovative life-sustaining **IoMT** for Fortune 500 biotech manufacturer

Secure communication with implanted connected pacemaker



Case Study



Challenge

- **A large medical device manufacturer** developing a bluetooth-enabled pacemaker required strong security in a global deployment.
- The enterprise needed to easily, quickly, and securely update a large number of implanted devices anywhere in the world with fair amount of data.
- Required FDA Class III certification for devices that support or sustain human life.



Solution

- **FIPS 140-2 Level 3 Thales Luna Hardware Security Modules (HSMs)** combined with Keyfactor Control provided an innovative solution.
- Implemented secure device credential issuance, firmware code signing and verification, and code signing private keys.
- Public key and root of trust were installed on the Internet of Medical Things (IoMT) devices, which would send encrypted patient data that could only be decrypted on Luna HSMs in the manufacturer's datacenter.



Results

- **Enabled innovative product manufacturing** and deployment by maintaining medical data safety and ensuring data is encrypted at rest and in motion.
- **Enabled secure updates with end-to-end secure communication**, increasing device effectiveness and life-span and enhancing patient's prospects.
- **Delivered operational cost savings** by consolidating Luna HSMs on-premises and in the cloud using Luna Cloud HSMs on **Thales Data Protection on Demand (DPoD)**.



Accelerate secure cloud migration in EMEA

Zero trust access control and authentication
for cloud services

Case Study



Challenge

- **Thousands of health care professionals working remotely** needed access to sensitive patient records.
- They required secure access through a variety of endpoints including personal tablets, laptops, and smart and legacy cell phones.
- Also required secure access to sensitive data in applications such as **Office 365 and Citrix**.



Solution

- **SafeNet Trusted Access** was integrated to provide secure multi-factor authentication access to **Microsoft Azure AD** and **Citrix Digital workspace**.
- Employees were able to use the authentication method that best suited their environment.
- Smart phones use OTP push solution; legacy mobile phones use SMS OTP; and others use SafeNet OTP 110 hardware tokens.



Results

- **Accelerated secure migration** to the cloud with integration of SafeNet Trusted Access done in hours.
- **Achieved significant savings** on on-premises infrastructure, maintenance, patching, and support with cloud-based solution.
- **Enjoyed better productivity and low maintenance** with fully automated token management and reporting features.
- **Ensured scalability with flexible policy and federation** capabilities that allow the addition of new cloud applications within minutes.

Reduce risk and complexity

Simplify compliance with centralized data and identity security governance



Discover and classify data across hybrid IT according to sensitivity to specific legislation requirements

Automate data protection with centralized policy-based enforcement from a single pane of glass

Apply data privacy and sovereignty rules through granular data and access security controls



nucleushealth™

Enhanced clinical collaboration and HIPAA compliance for Nucleus Health

Protection of medical images in cloud-based platform for global access



Challenge

- **NucleusHealth** advances care through cloud-based medical image management, allowing global access to images by health providers.
- The company required a fully automated, enterprise-grade solution that could handle enormous amounts of data and protect from zero day exploits, internal and external intrusions, and unauthorized access.
- Desired a central console to define and audit security policies across Hybrid IT for HIPAA compliance.



Solution

- **CipherTrust Transparent Encryption** with centralized key management enabled the protection of data across multiple systems, including **Mongo DB** and **Microsoft Azure**.
- Automated data security policy-setting, reporting, and regulatory compliance auditing.
- Provided a complete separation of administrative roles with role-based access control, allowing only authorized users access to patient data.



Results

- **Dramatically improved HIPAA compliance** posture with automated and centralized data security governance.
- **Provided scalability** to support cloud-based platforms and protect petabytes of data without impacting service level agreements (SLAs).
- **Enabled a sophisticated cloud-based dev-ops environment** with automated reporting, policy-setting, and audit traceability while keeping data protected even from root-level access.

Vanderbilt University prevents employee identity theft and comply with regulations

Protection of access to human resources and electronic prescriptions systems

VANDERBILT UNIVERSITY
MEDICAL CENTER

Case Study



Challenge

- **Vanderbilt University** decided to add multi-factor authentication throughout their organization after being plagued with phishing emails almost daily,
- With employees' email login credentials, hackers could access the human resource departments and attempt to get a hold of their bank account information, automatic deposit of paychecks information, and social security numbers.



Solution

- **SafeNet Trusted Access** Thales' cloud-based authentication solution was chosen, along with **SafeNet MobilePASS**, for both software and hardware options.
- Enabled the customer to add multi-factor authentication (MFA) to access sensitive applications.
- Users were able to use a smart phone enabled with the SafeNet MobilePASS app or a hardware token for authentication



Results

- **Prevented most security breaches** and mitigated the risk associated with identity thefts, including wider data breaches from stolen employee credentials.
- **Mitigated compliance risk with DEA rules** by strengthening security on systems for electronic prescriptions of controlled substances.
- **Provided flexible form factors** for authentication enabling the organization to reach all employees with authentication tools.

THALES

Protection of highly sensitive CCTV data to ensure HIPAA compliance

Protection of sensitive patient monitoring video feeds in e-health initiative



Challenge

- **An integrated healthcare system of hospitals** used an AvaSys closed-circuit TV (CCTV) to monitor patients and improve service and care.
- But sensitive patient video feeds were not being protected from intrusion, manipulation, or capture raising privacy concerns and putting at risk HIPAA compliance.
- The technology used to secure the video feeds would have to have extremely high performance to ensure video quality to recognize high risk health events in real-time.



Solution

- **Thales CN4010 Network Encryptor** was implemented to encrypt data flowing from cameras to all the way to monitoring stations.
- Sensitive data protected by NIST (AES-256) cryptographic algorithms and FIPS 140-2 Level 3 appliances at all endpoints.
- Thales Network Encryptors provide the fastest network encryption available high availability features support 99.99% uptime.



Results

- **Ensured end-to-end protection** for sensitive data from each camera all the way to the desktop monitoring system preventing most security vulnerabilities.
- **Mitigated privacy concerns** and dramatically enhanced its security posture towards HIPAA compliance.
- **Enabled high performance** of a large number of encrypted video feeds and ensured scalability with drop-in design able to support hundreds of concurrent encryption connections.

Thales Cloud Protection & Licensing

Our Solutions

Data Protection

Access Management &
Authentication

Software Monetization



Over **2,600**
employees



25 countries
presence



750 engineers
worldwide



30,000
customers worldwide

Thales's technologies and services help secure **more than 80%** of all global payment transactions and increasingly valuable corporate and government information.

The people we rely on to secure
our privacy rely on Thales

#1

Worldwide in
general-purpose
HSMs

#1

Worldwide in data
encryption

#1

Worldwide in
payment HSMs

#1

Worldwide in key
management

#1

Worldwide in
cloud HSMs

#2

Worldwide in
cloud
authentication

#1

Worldwide in
software
protection

#1

Worldwide in
software licensing


THALES

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data.



When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.



Decisive technology for decisive moments.



Contact Us

For all office locations and contact information, please visit



cpl.thalesgroup.com/contact-us



cpl.thalesgroup.com