eBook

THALES
Building a future we can all trust

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

cpl.thalesgroup.com

Healthcare & life sciences advance digital transformation

Healthcare, biotech and pharmaceutical organizations have been rapidly adopting new technologies and platforms to better serve customers win competitive advantages.

Cloud adoption

The global healthcare cloud computing market size was valued at USD $54.28 billion in 2024 and is projected to grow to USD $197.45 billion by 2032, exhibiting an annual growth rate of 17.6%.[1]

Big Data usage

Global Big Data in healthcare market size is expected to be worth around USD $145 billion by 2033 from USD 42.2 billion in 2023, growing at a annual rate of 13.2%.[2]

Artificial Intelligence (AI) usage by physicians

66% of physicians reported using health care AI in 2024 to the AMA for documentation of billing codes, medical charts, visit notes, creation of discharge instructions, care plans, translation services, assistive diagnosis and more.[3]

Artificial Intelligence usage by organizations

27% of healthcare & life sciences organizations said they are in the "integration" or "transformation" phases of their GenAI journey, according to the 2025 Thales Data Threat Report Healthcare & Life Sciences Edition.[4]

$197B

is the forecast **spent on public cloud** by healthcare firms by 2032

$145B

is the forecast **spent on Big Data** by healthcare firms by 2033

2 in 3

physicians reported using health care **Artificial Intelligence** in 2024 by the AMA

27%

are in the integration or transformation phases of their **GenAI journey**

1: Fortune Business Insights: : Healthcare Cloud Computing Market Size.
2: US Market News: Big Data In Healthcare Market Reaching US$ 145.8 Billion By 2033.
3:American Medical Association (AMA): 2 in 3 physicians are using health AI.
4: 2025 Thales Data Threat Report Healthcare & Life Sciences Edition.

THALES
Building a future we can all trust

Digital transformation increases complexity challenges

Digital transformation at healthcare & life sciences increases the complexity of hybrid IT infrastructure and the risk of data breach.

77

is the **average number of SaaS applications** and 1.9 for IaaS platforms.

32%

Use 500 or more **APIs**, 22% use 1,000 or more.

27%

have **little or no confidence** in identifying **where their data is stored**

Only 4%

have **encrypted** 80% or more of their **sensitive cloud data**

A challenging multi-cloud world

The average number of SaaS applications in use by healthcare & life sciences organizations is 77, while the average number of IaaS platforms is 1.9, highlighting the growing complexity of their multi-cloud environments.[4]

API Sprawl

32% healthcare & life sciences organizations use more than 500 APIs, and 14% use more than 1,000 across their environments.[4]

Data Vulnerability

22% of healthcare & life sciences organizations have little or no confidence in identifying where their data is stored.[4]

Lack of protection for sensitive data

Only 4% of healthcare & life sciences organizations have encrypted 80% or more of their sensitive cloud data, even as the proportion of sensitive cloud data increases.[4]

4: 2025 Thales Data Threat Report Healthcare & Life Sciences Edition.

THALES
Building a future we can all trust

The threat landscape, inside and out

Rates of recent data breaches among healthcare & life sciences organizations have steadily decreased, while breach complexity and sophistication continue to increase.

Data breaches

12% of healthcare & life sciences organizations reported a recent breach in 2025 down from 37% in 2021, but complexity of breaches increases.[4]

Breach causes

The top root causes of breaches are misconfiguration or human error, exploitation of known vulnerabilities, and identity failure or compromise.[4]

AI vulnerabilities

Concerns about the risks of deploying AI are growing, 69% cited the fast-moving AI ecosystem as their top concern, followed by concerns about lack of model and data integrity (65%) and trustworthiness (60%).[4]

The average cost of cyber attacks

The average cost of a cyber attack in the healthcare sector reached US$7.4M in 2025 according to the Ponemon Institute. The largest share of the cost is composed of lost business and reputational damage.[5]

4: 2025 Thales Data Threat Report Healthcare & Life Sciences Edition
5: Ponemon & IBM: Cost of Data Breach Report 2025

12%
Of organizations reported **a recent breach in 2025**

1st
The top root causes of breaches are **misconfiguration or human error**

69%
cited the **fast-moving AI ecosystem as their top concern**

$7.4m
The **average cost of a cyber attack** in the financial services industry

THALES
Building a future we can all trust

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 critical infrastructure security while enabling innovation and resiliency by protecting sensitive data, applications and identities.

Application Security

Protect applications and APIs with precision from bots, DDoS, and supply chain attacks and increase resilience and speed of your websites.

Data Security

Identify, protect, monitor, report, and govern sensitive data across hybrid IT, get real-time observability of threats with actionable insights.

Identity & Access Management

Orchestrate frictionless, secure, and trusted digital journeys for customers, employees, and partners at scale.

Application Security

Protect applications and APIs at scale in the cloud, on-premises, or in a hybrid model.

DDoS Protection

Maximize network and application availability with fast response to network and L7 DDoS attacks

Web Application Firewall

Web Application Firewall (WAF) Protects applications out of the box with near zero false positives

Client-Side Protection

Prevent data theft from client-side attacks like formjacking, digital skimming, and Magecart

Bot Protection

Protect website, mobile apps, and APIs from automated attacks

API Security

Protects APIs and API Data anywhere

Runtime Protection

Always on Zero Trust protection for applications

Managed DNS

Uninterrupted DNS resolution filters out bad traffic to only respond to legitimate requests

Secure CDN

Content caching, load balancing, and failover to securely deliver applications across the globe

Account Takeover

Prevents against automated account takeover fraud

Electronic Medical Records organization stops attacks with Application Security

Cloud WAF enables HIPAA Compliance and DDoS Protection

Challenge

- **Electronic Medical Records (EMR)** provider prides itself on offering a vast set of applications with scheduling, documentation, billing, and clinical reporting capabilities.
- The company faced frequent large-scale hacker attacks and attempts at stealing highly sensitive medical data, negatively impacting IT staff.
- Needed a solution against large-scale attacks, stop data theft and site scraping, while ensuring 24/7 site availability to its users and maintaining HIPAA compliance.

Solution

- **Cloud Web Application Firewall (WAF)** was quickly deployed to protect essential applications from a range of attacks including intruders, DDoS traffic, and scraping bots.
- With automatic DDoS mitigation SLA of 3-seconds or less for any type, size, or duration of attack, the company is covered against even the most powerful DDoS attacks with an industry-best guarantee.

Results

- **Improved speed of DevOps** by deploying new patches and new versions in just days and weeks, rather than months.
- **Increased visibility** with real-time monitoring displaying number of attackers being blocked, the reasons for blocking them, geographical sources of hostile traffic and more.
- **Reduced burden** on the company's IT team by automatically deploying security updates and upgrades across the network and having intelligence at their fingertips.
- **Improved compliance** posture with regulations such as HIPAA by enabling swift protection of systems and privacy of personal medical data.

Data Security

Identify, protect, monitor, report, and govern sensitive data across hybrid IT.

Our Data Security Portfolio


Data Discovery & Classification


File, DB, & App. Encryption


Enterprise & Cloud Key Management


Secrets Management


Tokenization & Data Masking


Data Governance & Monitoring


Threat Detection & Response


Hardware Security Modules


High Speed Encryption

Protects Anything


Personal Information


Intellectual Property


Internet of Things


Customer data


Enterprise data


Financial data

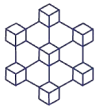

Secrets & credentials

Anywhere

Applications


Data centers


Containers


Networks

Virtual


Clouds


Big data

Click to learn more about our Data Security solutions

Fortune 100 healthcare enterprise ensures customer trust in the highly-regulated healthcare industry

HIPAA compliance and protection of PHI in Hybrid IT with **CipherTrust Platform**

Challenge

- **A Fortune 100 healthcare enterprise** focused on the development and delivery of drugs and healthcare products, needed a solution 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.'

Protect sensitive patient data for for large healthcare organization

Data Security Fabric protects 780 database servers and 15 critical applications

Challenge

- **A large healthcare organization** with dozens of hospitals and medical centers in six states needed to balance access to patient data against the risk of a data breach.
- Patient data is used at every step of the patient care experience, resulting in a sprawling environment that spans structured and unstructured data, and data stored in the cloud.
- While starting a multi-year cybersecurity protect the company was breached. The organizations realized it needed a data-centric approach to protect data immediately.

Solution

- **Data Security Fabric** was quickly deployed to protect the "Crown Jewells" of the company, the most sensitive patient data in critical databases and applications.
- Data Security Fabric provides automated dashboards and reports, making it easy to pull reports on who is accessing a given database for a specified time range. Those reports also make it easy to demonstrate compliance.

Results

- **Quick time-to-protection**, 20 key database servers were quickly protected while the security team built the architecture to support the full deployment of 15 business-critical applications and over 780 database servers.
- **Increased visibility** by monitoring data access and detecting threats in real time with automated dashboards and reports.
- **Saved millions of dollars** in Splunk SIEM license fees by using machine learning and behavior analytics to distill 45 billion event alerts per day down to 150 critical alerts.
- **Ready for the future**, with a scalable solution able to handle new applications and environments as the business evolves.

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

Protection of implanted connected pacemaker connections with **HSMs**

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).**

Protection of highly sensitive CCTV data to ensure HIPAA compliance

Protection of sensitive data in motion with **high-speed encryption**

Case Study

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.

Enhanced clinical collaboration and HIPAA compliance for Nucleus Health

Protection of medical images for global access in the cloud with **CipherTrust Platform**

Case Study

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.

Identity & Access Management

Provide seamless, secure and trusted access to applications and digital services.

Identify

- Bring Your Own Identity (BYOI)
- Document Verification, Liveness Detection

Authenticate

- Digital ID Wallets, Mobile ID, Digital Driver's License
- SCA, Phishing-resistant Authentication,
- Single Sign-on, Passwordless

Authorize

- Adaptive Access
- Fine-grained Authorization
- Delegation and Relationship Management

Delete

- Account Deletion
- Right to forget

SIGN UP → **LOG IN** → **USE** → **LEAVE**

Workforce & Customer IAM - User Journey & Consent

- User Journey Orchestration, Authentication Journey
- Consent and Preference Management
- Progressive Profiling

Multi-Factor Authentication

- PKI CBA
- OTP Hardware
- fido

Accelerate secure cloud migration in EMEA

Zero trust access control and authentication for cloud services with **SafeNet Trusted Access**

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.

Vanderbilt University prevents employee identity theft and comply with regulations

Protection of access to human resources and electronic prescriptions systems

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 Benefits

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, application and **identity protection** with **scalable** solutions for multiple use cases

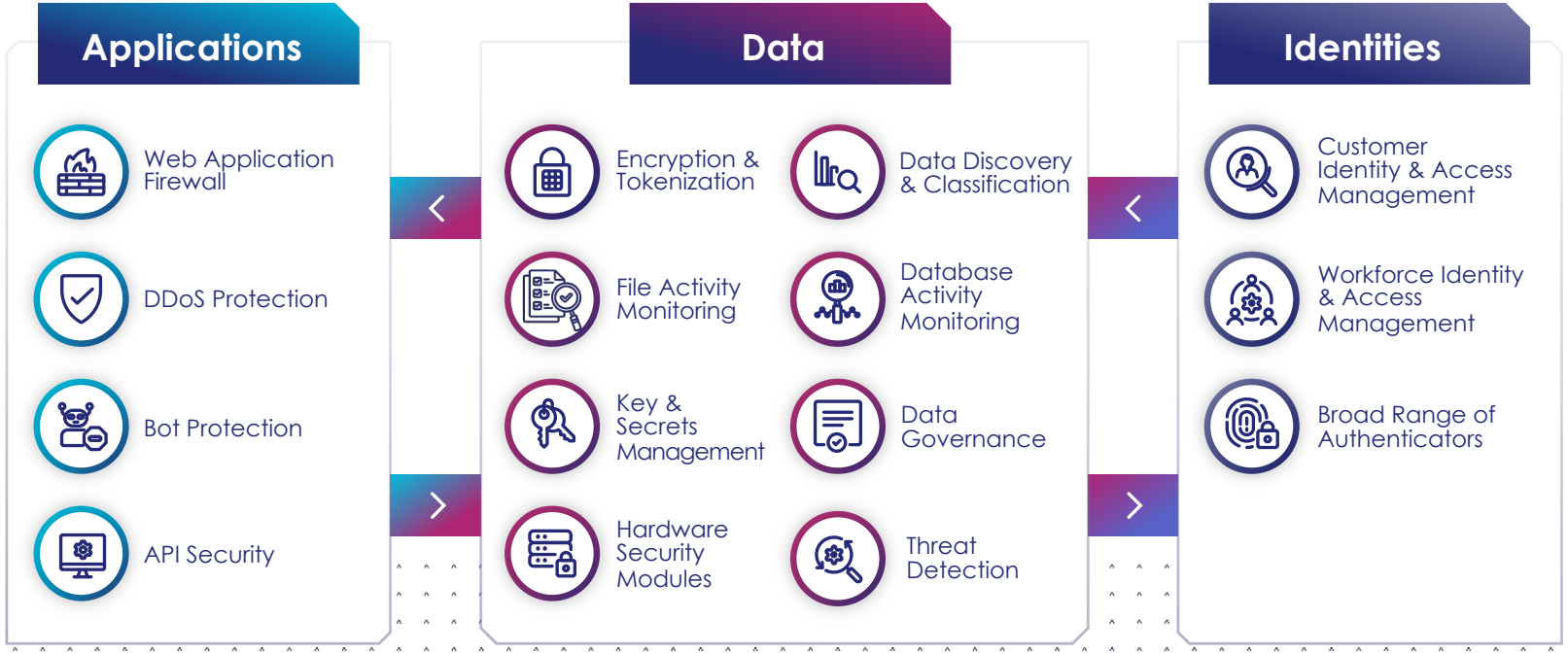
Accelerate digital transformation

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

Thales reduces the complexity of compliance with platforms that protect and manage applications, data, and identities at scale



Thales Cybersecurity at-a-Glance

~6,000 employees worldwide & **€2 billion** in revenue

30,000+ Customers Worldwide

6,700+ Partners Worldwide

Leader in **Forrester WAVE for Web Application Firewall Solutions 2025**

Overall Leader in **KuppingerCole Leadership Compass for Data Security Platforms 2025**

Visionary in **2024 Gartner Magic Quadrant for Access Management**

Next steps

Learn More

Web page:

Data Security Solutions for Healthcare & Life Sciences

Analyst report:

Data Threat Report Healthcare & Life Sciences Edition

Solution brief:

Imperva for Health Care: Securing Positive Patient Outcomes

Contact Us

> Schedule a demo
> Learn more about our use cases
> Talk to a representative

About Thales

Thales is a global leader in data security, trusted by governments and the most recognized companies around the world to help them protect their most sensitive data. 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.

THALES

Building a future we can all trust

Contact Us

For all office locations and contact information, please visit

cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com