

eBook

THALES
Building a future we can all trust

Securing Critical Infrastructure while Enabling Innovation, Transformation, and Resiliency

cpl.thalesgroup.com

The next generation of critical infrastructure relies on innovation

Technological innovation is driving the next generation of critical infrastructure, allowing enterprises to improve service, optimize operations, and ultimately deliver better value to stakeholders



Gather

Gather valuable information through sensors, cameras, and drones throughout the infrastructure footprint.

Communicate

Communicate data in real time through IoT and other connected systems.

Aggregate

Aggregate data in central management consoles to automate remote production or distribution facilities.

Analyze

Analyze data in big data repositories and leverage artificial intelligence (AI) to power better decision making.

Optimize

Optimize operations by acting on insights quickly using all digital controls to manage distributed infrastructure such as "Smart Grids".

Deliver

Deliver on commitments to customers with digital customer experience, better reliability, lower cost, and adoption of renewables.



Utilities and energy industries advance digital transformation

Critical infrastructure sectors, such as utilities and energy, are adopting new platforms and environments at a fast pace, transforming the capabilities of both their Information Technology (IT) and Operational Technology (OT) platforms.

Spending on Internet of Things (IoT)



Spending on Internet of Things (IoT) in the utilities sector is set to grow to US\$ 129.1 Billion by 2032, providing connectivity and a host of new possibilities to a widely distributed infrastructure.¹

Artificial Intelligence (AI)



Artificial Intelligence (AI) usage in the energy industry is expected to grow 22.9% a year in the energy sector, helping increase efficiency and automate decentralized power generation.³

Big Data analytics



The Big Data analytics market in the energy sector is expected to grow 69% by 2029, allowing enterprises to gain insights faster for better decision making and competitive advantages.²

Cloud adoption



A majority of utilities and energy companies have 40% or more of their data in the cloud, helping advance customer experience, and address the needs of data management and processing.⁴

\$129B

is the estimated spending on **IoT** by Utilities by 2032

69%

Increase in **Big Data** spending until 2029



22.9%

CAGR of **AI** spent in the energy sector

40%

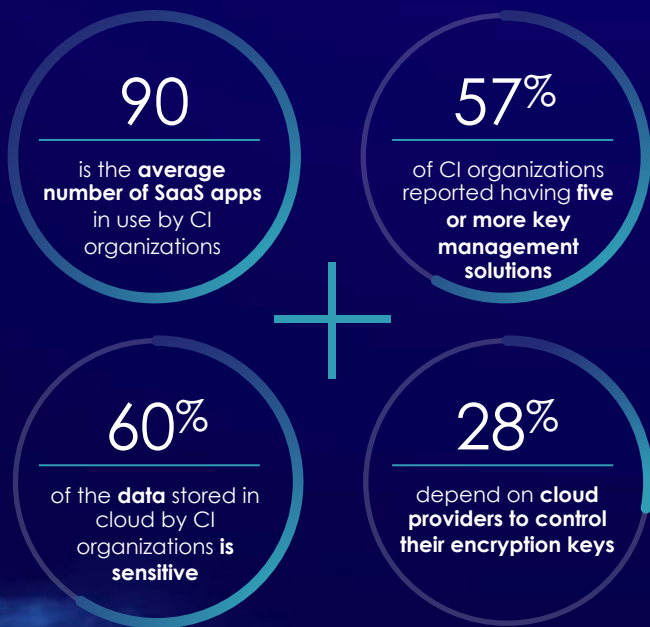
or more of their data is in the cloud for a majority of utilities

1: Future Market Insights: IoT In Utilities Market Outlook (2022 to 2032)

2: Mordor Intelligence: Big Data Analytics Market in the Energy Sector (2024-2029)

3: Future Data Stats: Artificial Intelligence in Energy and Utilities Market Size (2023-2030)

4: Thales Data Threat Report Critical Infrastructure Edition 2024



Digital transformation increases complexity challenges

Digital transformation at critical infrastructure (CI) organizations increases the complexity of hybrid IT infrastructure and the risk of data breach.

A challenging multi-cloud world



The average critical infrastructure organization has 90 Software-as-a-Service (SaaS) providers, and two or more Infrastructure-as-a-Service (IaaS) providers.⁵

Key management complexities



57% of critical infrastructure organizations reported having five or more key management solutions, increasing complexity and making it cumbersome (and expensive) to manage.⁵

Cloud sensitive data



Critical infrastructure organizations reported that 60% of their data stored in the cloud is sensitive.⁵

Lack of separation of duties



28% of critical infrastructure organizations depend on cloud providers to control their encryption keys for more than half of applications.⁵

Hacker groups target weaknesses in critical global infrastructure

The devastating cyberattack that derailed a pipeline operator for a week and impacted 45% of the U.S. East Coast's fuel supply in 2020 was an eye opener for the broader public as to the vulnerability of the critical infrastructure sector.

Cyber attacks



9 out of 10 critical infrastructure organizations have experienced an increase in attacks, with 42% acknowledging being breached at some point.⁵

Malware



The top threat to critical infrastructure organizations continues to be malware, followed by phishing and ransomware.⁵

Ransomware attacks



23% of critical infrastructure organizations have experienced a ransomware attack, however only 1 in 7 said they would follow a formal plan in the event of an attack.⁵

The average cost of cyber attacks



The average cost of cyber attacks in the energy sector in 2023 reached US\$4.78M according Ponemon Institute cost of data breach report. The largest share of the cost is composed of lost business and reputational damage.⁶

9 out of 10

CI organizations have experienced an increase in attacks

1st

Malware is the number one threat to CI organizations



23%

have experienced a ransomware attack

\$4.78m

was the average cost of a cyber attack in the energy sector

Stricter cybersecurity mandates and legislation add urgency

The growth of cyber incidents at critical infrastructure organizations has led to unprecedented executive and legislative action:



White House Cybersecurity
Executive Order



Network and Information
Security Directive (NIS) 2

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 critical infrastructure organizations to secure cloud services and a zero-trust architecture and mandates deployment of multi-factor authentication and encryption.

The European Union's NIS 2 requires operators of critical infrastructure and essential services in the EU to implement appropriate security measures and report any incident to the relevant authorities. The Directive includes stricter security and risk management requirements, reporting obligations, and introduces more stringent supervisory measures, including harmonized sanctions across the EU.

Because of the convergence of existing privacy, sovereignty, and data protection regulations, such as GDPR and PCI-DSS; federal standards, such as FedRAMP and FIPS; global standards, such as ISO 27001, and operational best practices such as SCADA; critical infrastructure organizations are faced with a comprehensive set of rules that make compliance much more complex and challenging.

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 at scale in the cloud, on-premises, or in a hybrid model.

Data Security



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

Identity & Access Management



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

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

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

[Click to learn more about our Application Security solutions](#)





Ensuring application availability for major European power company

Safeguard customer access and preserve infrastructure resources



Challenge

- **A major European power company** was focused on ensuring the security and privacy of all its customer interactions through its website and applications.
- The organization wanted to ensure the protection of its most important web applications from external attacks such as DDoS and OWASP.
- In addition, new account takeover attacks and credential-stuffing, involving millions of malicious requests, taxed the security team and rendered defenses ineffective.



Solution

- **Web Application Firewall (WAF)** was deployed to protect essential applications from DDoS and other types of attacks.
- **Account Takeover Protection (ATP)** addressed malicious login attempts while maintaining a seamless user experience.
- Using a multilayered approach, ATP is able to determine if interactions have the characteristics of an account takeover in order to stop attacks from the first request.



Results

- **Deflected 22.5 million malicious requests** during a 3-day account takeover attack while allowing uninterrupted access for customers.
- **Increased resiliency**, maintaining unwavering availability of websites and mobile apps, even amidst major attacks.
- **Enabled continued to compliance** with privacy and security regulations in the European Union by protecting customer data and customer access.
- **Easy out-of-the-box onboarding** enabled swift protection of systems.



Increased critical app resilience against attacks for SA Power Networks

Protection for essential web applications, API endpoints and compliance with regulations



Challenge

- **SA Power Networks**, as a key player in South Australia's energy industry, needed to ensure the resilience of its services in the face of growing cyber attacks.
- The utility was especially concerned about the protection of its web applications from attacks such as distributed denial of service (DDoS) and the vulnerability of exposed APIs.
- In addition, the Security of Critical Infrastructure (SOCl) regulation mandated the utility's protection of customer access to power and protection of customer data.



Solution

- **Web Application Firewall (WAF)** was deployed to protect essential applications from DDoS and other types of attacks.
- **API Security** was deployed to automatically detect and classify API endpoints, identifying vulnerabilities and establishing required safeguards.



Results

- **Deflected 18.5 million malicious attempts** during a relentless 3-day DDoS attack aimed at SA Power Networks digital infrastructure, preventing service disruption and maintaining operations.
- **Provided visibility to security teams**, equipping them with measurable metrics, including number of potential attacks and API endpoints detected and prevented.
- **Enabled continued to compliance** with privacy and security regulations including SOCl.
- **Integrated with seamlessly DevSecOps practices**, allowing the company to bolster its security while promoting agile development and deployment practices.

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](#)



Protecting tier 1 data across Hybrid IT for global energy provider

Protecting high value data on-premises and in the cloud



Challenge

- **A highly regulated global energy company** with operations in multiple countries needed to protect high-value data across multiple platforms.
- Even though the customer already had advanced security, it wanted the highest level of security for its most sensitive “tier 1” data to protect against not only external attacks, but also insider privilege abuse and government subpoenas.
- The customer also needed to ensure no downtime when protecting production data.



Solution

- **Thales CipherTrust Transparent Encryption** was deployed to protect a wide variety of file formats and data stores.
- Granular controls allowed only specific data to be decrypted when needed by authorized users while keeping encrypted all other data, whether on-premises or in the cloud.
- **CipherTrust Live Data Transformation** allowed the energy company to protect production data with minimum downtime.



Results

- **Addressed Federal Energy Regulatory Commission (FERC)** and GDPR regulatory requirements as well as global and regional mandates and standards.
- **Achieved protection in the cloud** against subpoena or external and internal threats with Bring Your Own Encryption (BYOE) platform for multiple cloud instances.
- **Enabled the protection of live data** without moving databases offline for critical systems with large and essential datasets, such as SAP Hana on premises and in the cloud.



Secure transition to country-wide Smart Metering in Europe

Protection of IoT devices and personal information on databases and file servers



Challenge

- **A major European energy utility organization** was transitioning most of the country's subscribers to connected smart meters.
- This highly regulated utility needed to comply with strict department of energy requirements for cybersecurity and data privacy, from the product design phase through implementation and systems management.
- The organization required a strong, reliable, and scalable security infrastructure that would support mandated cryptographic algorithms based on a FIPS140-2 Level 3 HSM.



Solution

- **Thales Luna Hardware Security Modules (HSMs)** were deployed to secure all PKI certificate authentication, code and device signing for millions of smart meters.
- The Luna HSMs, run the mandated algorithm and manage and generate high entropy keys in a FIPS 140-2 level 3 environment and enable management of keys independently from service providers.
- **Ciphertrust Manager** was also implemented to encrypt in databases and file servers sensitive personal data from millions of subscribers.



Results

- **Achieved audit compliance** with energy industry and GDPR regulations for both security and privacy.
- **Improved overall resilience** of energy infrastructure by protecting smart meter connections at millions of homes and businesses.
- **Successful roll out led to expansion** into personal information protection using encryption and key management.
- **Ensured high performance and scalability** able to support millions of devices and encryption keys.



Securing migration to the cloud for global energy leader

Managing and securing encryption
keys for major cloud deployment



Challenge

- A **global energy industry leader** was migrating the bulk of its datacenters to the cloud and needed to secure sensitive data to comply with regulations.
- Hundreds of Microsoft Azure subscriptions, each with several key vaults presented a huge level of complexity for managing keys.
- The customer wanted a vendor-agnostic solution able to manage and store keys on premises for multi-cloud deployments leveraging the bring your own key (BYOK) model.



Solution

- **Ciphertrust Cloud Key Manager (CCKM)** was deployed by the customer to manage encryption keys from a single pane of glass across all Azure subscriptions.
- CCKM provided the customer with simplified management and control over BYOK keys managed on-premises.
- FIPS 140-2 Level 3 hardware security modules (HSMs) guaranteed high entropy key generation and secure key storage.

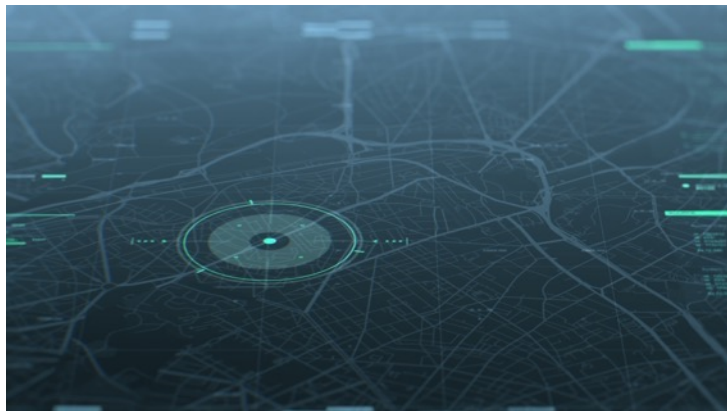


Results

- **Achieved complete visibility and control** over key management across multiple cloud subscriptions used by several business units and subsidiaries.
- **Automated key lifecycle management**, simplifying generation, rotation, backup, and revocation of millions of keys.
- **Enabled continued to compliance** with privacy and security regulations across multiple countries.
- **Ensured developer-friendly environment** with REST APIs allowing new applications to easily tap into CCKM for key management.

Protect critical communications for major energy operator

End-to-end high-speed encryption for critical data in motion during pandemic



Challenge

- **A major UK energy operator** needed to connect to other utilities via the National Grid Network.
- Data within the network is of critical national importance and mandates stipulate that the highest levels of security be deployed.
- High performance end-to-end encryption of data in motion was required to ensure data was secure.
- Deployment had to be done remotely because of the start of the COVID 19 pandemic.



Solution

- **Thales CN6010 High Speed Encryptors** were deployed by the energy operator to protect sensitive data in motion between the energy utility and the National Grid Network.
- The FIPS 140-2 Level 3 and Common Criteria CN6010 provided high speed communication with the highest levels of standards-based security.



Results

- **Protected sensitive data** communicated between the utility and the network and was able to immediately detect manipulated data packets and shut down compromised transmissions.
- **Improved overall resilience** of energy infrastructure by delivering large volumes of data at high speed for analysis and action.
- **Achieved quick deployment** by remotely designing, delivering, and deploying the solution within 3 months even with the COVID 19 pandemic in full swing.

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

[Click to learn more about our Identity
& Access Management solutions](#)



Access management & security for clean energy provider

Centralized access management with
MFA for critical distributed systems



Challenge

- **A North American clean energy provider** with major corporate customers needed a solution to protect its network of on-site fuel cell production facilities.
- As an energy utility, it needed to comply with cybersecurity mandates from the Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC).
- The company required a scalable, flexible and resilient multi-factor authentication (MFA) solution to protect access to distributed facilities.



Solution

- **Safenet Trusted Access** cloud-based IAM solution was chosen by the customer to protect VPN access to all critical assets and access points.
- Multi-Factor Authentication with convenient and flexible authentication methods added strong security while ensuring adoption and usability.
- Centralized access management allowed for granular access governance based on compliance and security requirements.



Results

- **Enforced centralized access management** and authentication to help compliance with energy industry regulations and mandates.
- **Achieved successful protection of critical systems** from external and internal threats, increasing resilience of critical energy production systems.
- **Allowed for expansion into access control management** for switches and other systems in an increasingly diverse IT infrastructure.
- **Currently expanding** number of users by 80%

Thales benefits

Thales enables critical infrastructure security while enabling innovation, transformation, and increased resiliency.

Accelerate
digital transformation



Offer better services by adopting innovations, such as IoT, Cloud, and AI faster with a framework for a zero-trust world

Increase
resilience and efficiency



Automate and streamline applications, data, and identity protection across cloud and on-premises systems

Reduce
risk and complexity



Simplify compliance and minimize reputational and operational risk with centralized app, data & access security governance

Thales Cloud Protection & Licensing at-a-glance



Next steps

Learn More

Web page:

Critical Infrastructure Solutions & Case Studies



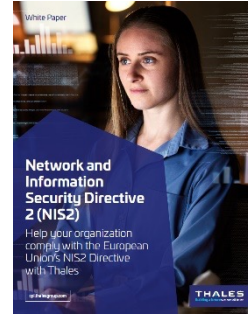
Analyst report:

Data Threat Report Critical Infrastructure Edition



White paper:

Compliance with the Network and Information Security Directive 2 (NIS2)



Contact Us



- > [Schedule a demo](#)
- > [Learn more about our use cases](#)
- > [Talk to a representative](#)


Contact 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