Ensuring safety in today's regulatory climate

How critical industries are addressing European regulatory requirements.

cybereason©

Introduction

In 2013, regulators in the EU set out the ambitious goal of making Europe the ‘safest online environment in the world’.

To do this, they launched a series of initiatives and regulations designed to keep citizens safe from bad actors online—mandating business cybersecurity readiness, codifying reporting requirements, and building resilient systems that can survive an attack.

Over time, these standards have evolved into the regulations we know today: CRA, GDPR, NIS and NIS2, mandating data privacy and protection.

In this document, you’ll see how three European organizations that provide critical services are complying with the regulations while protecting their operations with the only effective on-premise security solution on the market. These are Cybereason customers operating in highly sensitive and regulated sectors; for this reason, we cannot provide full details.

▶ There is also an additional use case document in this series, which looks at the technological hurdles facing industry leaders as they strive to protect privileged information using Cybereason’s state-of-the-art tools.

Three organizations: three different challenges

As the EU develops their responses to the alarming growth of cyberattacks, businesses need to secure their own data while complying with a flurry of new laws.

Organizations across Europe are faced with regulatory demands that stress maximum uptime with operational resiliency. Each of these critical industries needed to take a strategic approach designed specifically for their unique challenges.

USE CASE

A LARGE ENERGY PROVIDER

Meeting the energy needs of hundreds of thousands of citizens requires that critical systems remain up and running at all times, and beyond the reach of online attacks. As an essential service, the level of regulation they face is very stringent.

This company's highly-regulated industry needs to report on efforts to secure their networks, ensure resiliency in the event of an attack, document any intrusions, and protect power generation facilities.

The existing Endpoint Protection (EPP) solution had no server-based detection capabilities. Solutions had to address group assets with limited network access, with subsidiaries in countries all over the world, and assets in restricted areas for nuclear activities.

- Cybereason On-Prem replaced the legacy EPP solution. Not only does it protect their servers, it provides an account of any incidents and allows a rapid response to any attack it discovers across the worldwide network.

USE CASE

GOVERNMENT-AFFILIATED ASSET MANAGEMENT GROUP

The finance industry is no stranger to regulation, and the data security provisions of current EU regulations are quite complex. Not only are there stringent data protection requirements, but data residency and reporting requirements are just as strict.

Maintaining customer transaction data onsite is a necessity, so they turned to the only solution providing state-of-the-art protection for their servers and storage.

Cybereason On-Prem allows the organization to keep their critical information protected with a single, class-leading EPP and EDR solution, completely disconnected from the internet.

USE CASE

PRODUCER OF GOVERNMENT DOCUMENTS

Tamper-evident and tamper-resistant physical documents are considered essential to maintain trust.

Allowing the production of those documents to be compromised by cybercriminals, or their unique countermeasures discovered and stolen by bad actors, is enough to keep a CISO up at night. Regulators maintain a close eye on the operations of these specialized industries.

Cybereason On-Prem keeps secret printing designs and paper formulations, as well as their industrial controls, in compliance and safely separated from the outside world.

Flexible deployments of Cybereason On-Prem have given these organizations onsite solutions that are completely air-gapped, without the need for an internet connection.

Machine learning allows vulnerabilities and threats to be proactively identified and sequestered in minutes. Solutions are presented in a single, easy-to-understand console, with the threats identified for swift action and documented for regulatory compliance.

Compliance: what you can do

Organizations serving critical societal needs have special obligations to their customers, shareholders, and the countries in which they reside.

Whether you're making the decision to retain your data on-premise, in the private or public cloud, or a combination, Cybereason can tailor a solution that helps you address the regulatory requirements you might encounter.

DATA SOVEREIGNTY

If you're located in a country mandating data storage and processing within its borders to protect a national interest, then Cybereason can protect your private network with the latest security solution without the need to connect your servers to the internet.

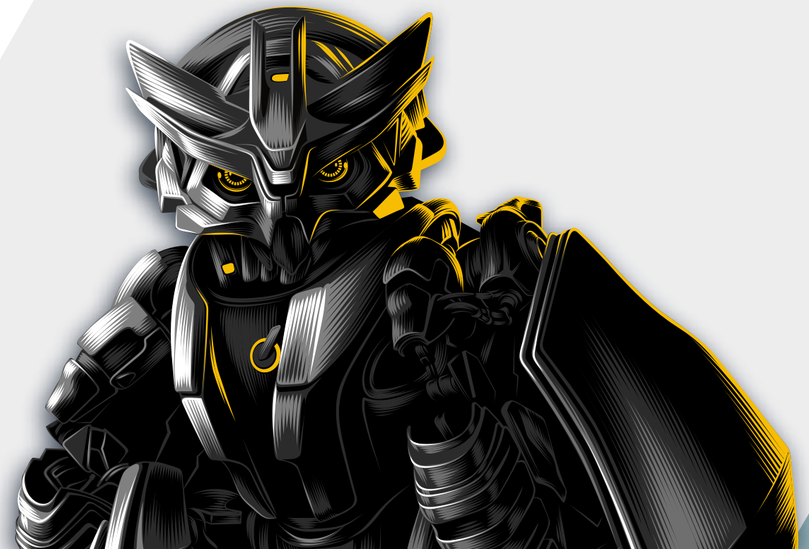
DATA RESIDENCY

Whether your data is stored in the public cloud or onsite, it may also be the subject of government regulation. If your industry is considered critical, or of special national interest, storing and processing data on a private, air-gapped network can be necessary to comply with local regulations.

DATA PRIVACY

Compliance with GDPR not only means documenting how data is collected, used, stored and shared, it's also critical to report on any network intrusions that might have compromised that data.

Cybereason tools can identify abnormal behavior on your network and document the path taken for any reporting.



DATA SECURITY

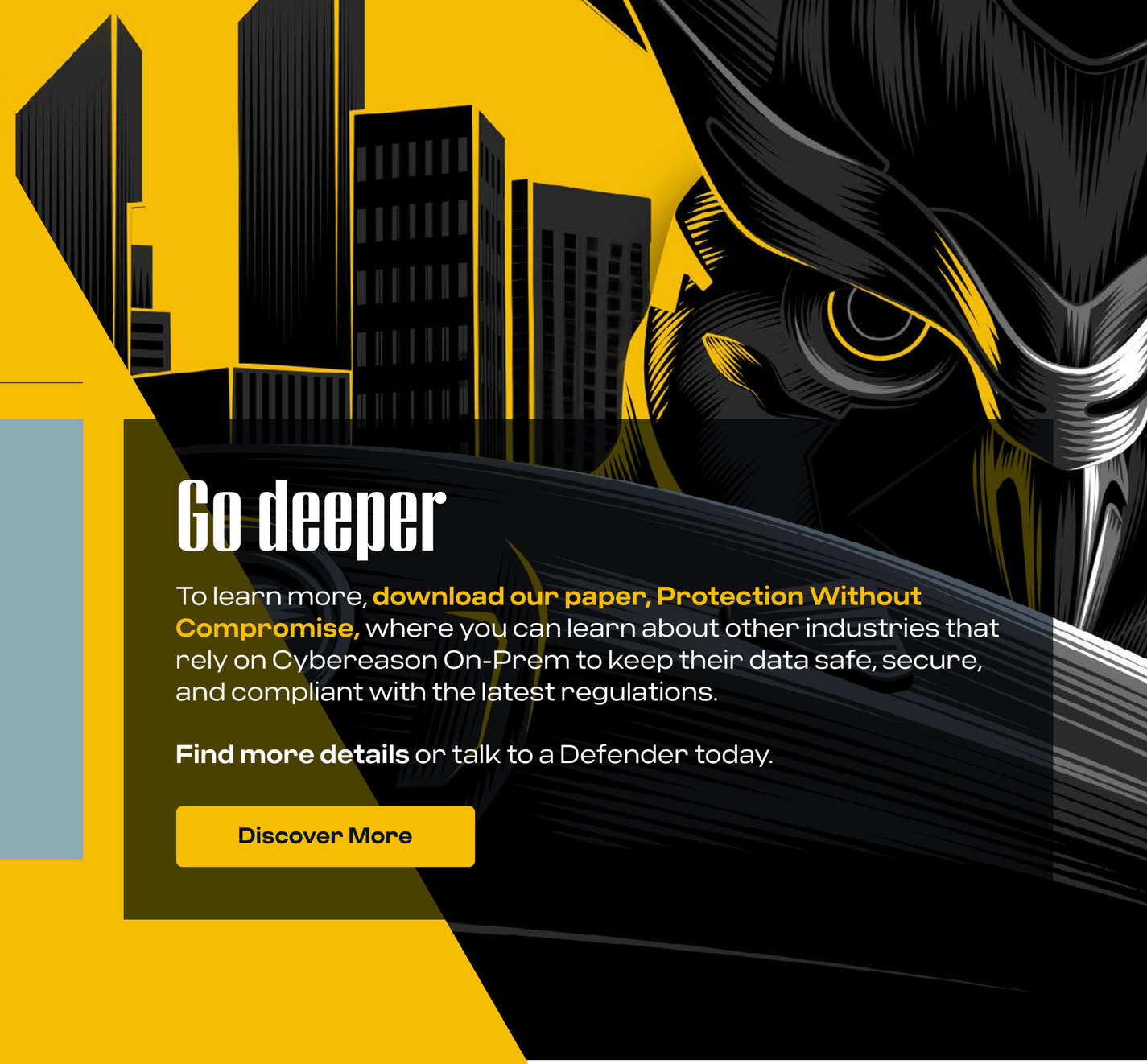
Cybereason protects data from unauthorized access, with multi-layered protection that encompasses software-driven antivirus, NGAV, EPP and EDR. Its machine-learning ability helps recognise attacker behaviour, their use tools and techniques and flag activity for further investigation.

Cybereason also provides the only platform on the market that reveals the complete history of an attack in real-time, automatically.

When the security team is notified of a malicious operation, they have a map of what has happened and who is affected. Guided or automated remediation can then be performed across all impacted devices with a single click. This is critical for compliance with compromise reporting requirements in the GDPR.

Cybereason On-Prem: proof positive

- **Undefeated** against ransomware
- Some of the **highest MITRE ATT&CK testing scores** ever recorded
- **Unprecedented network visibility** to detect threats
- **Reduced alerts** and false positives



Go deeper

To learn more, **download our paper, Protection Without Compromise,** where you can learn about other industries that rely on Cybereason On-Prem to keep their data safe, secure, and compliant with the latest regulations.

Find more details or talk to a Defender today.

Discover More

cybereason©

LEARN MORE AT CYBEREASON.COM