Evolving threats. New responses.

How organizations are adapting to a new breed of cybersecurity threats in a surprising way.

cybereason©

Introduction

GLOBALLY, CYBERCRIME CAUSES

€16 Million

IN DAMAGE EVERY MINUTE [1]

THAT'S

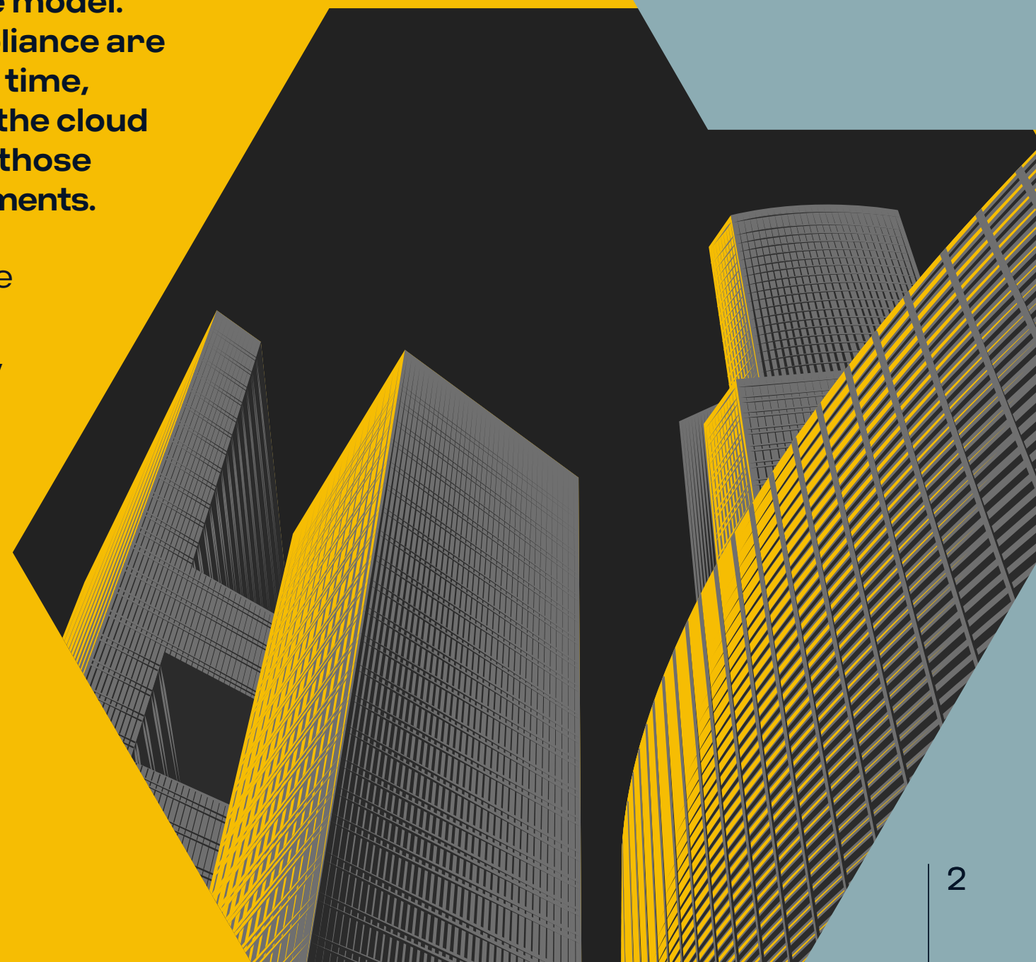
€8 Trillion

IN LOSSES THIS YEAR ALONE [1]

Government guidelines introduced to safeguard consumer data and protect critical infrastructure are challenging companies' desire to move to a Software-as-a-Service model. The risks of a failure of compliance are seen as too great. At the same time, endpoint solutions adapted for the cloud are struggling to keep pace with those ever-tightening regulatory requirements.

In this document, we look at how these challenges are affecting organizations that provide critical services, like utilities, government services and banks.

You can see how organizations are adopting new approaches to securing their networks, complying with regulations, and protecting their operations with the only effective on-premise security solution on the market.



[1] Cybersecurity Ventures - 2022 Official Cybercrime Report

The attackers: bad actors and hostile idealists

Cybercriminals can be anyone from an anonymous individual or a state actor, to a terrorist group, or an organized criminal gang. Their motivations range from purely financial, to ideological, or simply the notoriety of achieving a successful breach.

What they have in common is an evolving set of tools to compromise network security and create havoc.

An organization's planning and response to an attack, particularly if regulators consider the business to be critical, can determine whether services continue running and whether any sanctions are imposed.

Cybereason has been working with organizations around the world to help them answer some critical questions:

- Are key systems exposed to the public internet or running on a private network?
- Are the attackers' moves tracked and documented?
- How quickly is the attack recognized and stopped?

The customer use cases in this series show how Cybereason On-Prem is helping provide robust and compliant answers to these questions.

Compliance: the moving target

The pressure on CISOs overseeing critical IT infrastructure is mounting, especially in highly-regulated sectors.

In the EU, for instance, the Cyber Resilience Act has identified critical products that require a higher level of security and the NIS2 directive imposes a cross-border regulatory framework to set a baseline for risk management and reporting.

IT departments face data residency requirements, keeping specified datasets onsite and out of public cloud services, with an audit trail of threat detection and responses.

Data localization rules have already made migration to the cloud challenging. Even if the service provider could guarantee that a dataset resides in the statutory jurisdiction, documenting compliance is not straightforward.

Visibility is critical for this level of compliance. Organizations must show where data is stored and prove continuously that it is secure, and that defenses are compliant and effective.

The technology: a bold solution is needed

Eight billion people own at least one device that's connected to the internet. These endpoints are the most common entry points for criminals penetrating otherwise secure networks. Internal resources accessed from the cloud are a rich target, and only one password away from an attacker.

The obvious and most drastic solution is to completely cut off internet access to sensitive data stores and privileged information. **Governments and businesses have used an air-gapped approach to separate their most valuable data from the outside world for years.**

But over time, when servers need to be patched and applications need updates, temporary connections can inadvertently become permanent. Data stores begin to mingle and information can once again be vulnerable to attack.

Still, migrating legacy defenses to a modern deployment can be daunting, not least because of the lack of qualified cybersecurity professionals.

Institutions simply don't have the resources to devote large numbers of technicians to data protection, or the ability to modernize defenses on systems that aren't connected to the internet.

Taking action: how organizations are responding

In this use case series, you can see how organizations in some of the world's most commercially and geopolitically sensitive sectors have implemented effective on-premise EDR and NGAV. Cybereason keeps data on the perimeter, even when critical infrastructure is only partially air-gapped.

A LARGE ENERGY PROVIDER

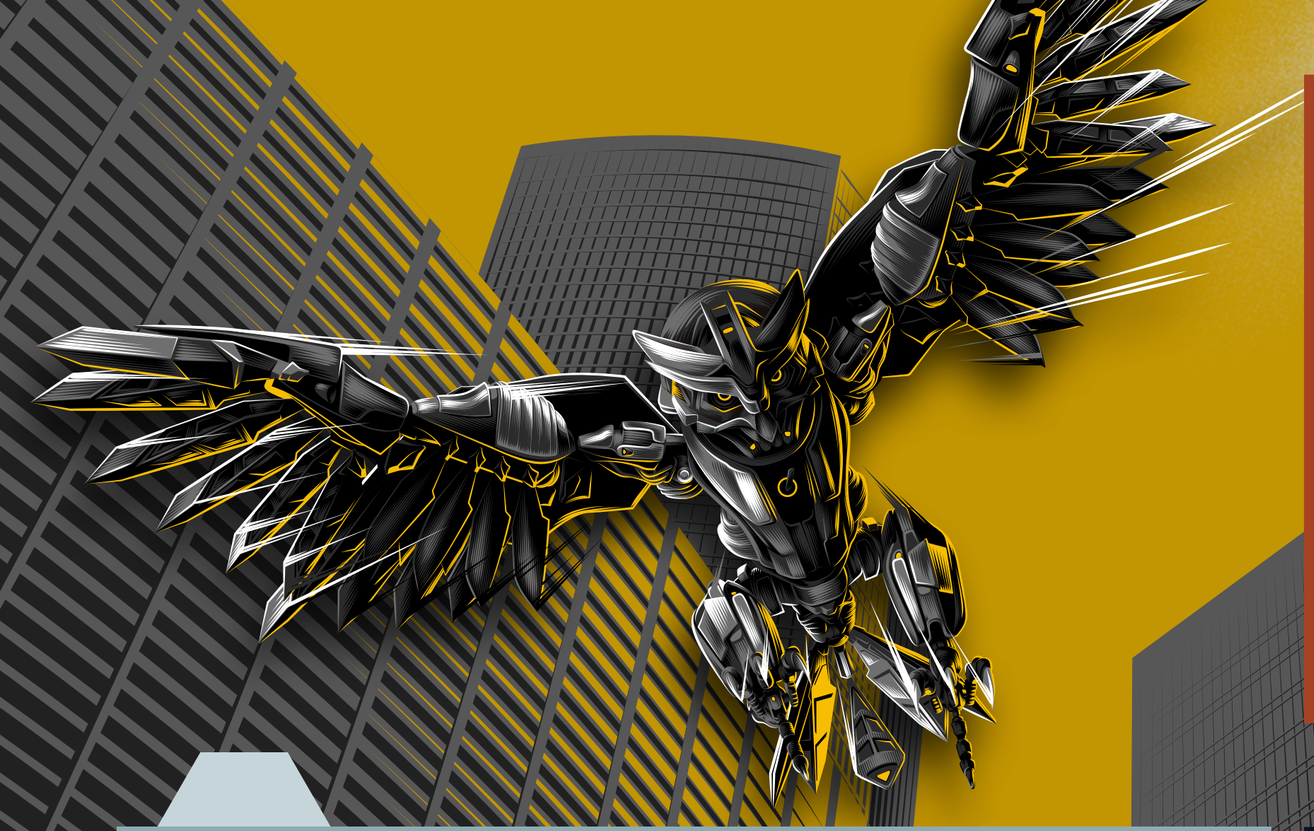
The business had an Endpoint Protection (EPP) solution that could not detect intrusions on its servers. A hybrid solution from Cybereason now combines on-premises protection for the servers with SaaS-based Endpoint Detection and Response (EDR) to protect workstations around the world.

GOVERNMENT-BACKED ASSET MANAGEMENT GROUP

The organization wanted to avoid a move to the cloud, with the accompanying mountain of regulatory obstacles, but were unaware of a compliant on-premise EDR solution. The unified EDR and EPP delivered by Cybereason On-Prem allowed them to implement their preferred strategy.

PRODUCER OF GOVERNMENT DOCUMENTS

Cybereason On-Prem keeps secret printing designs and paper formulations away from bad actors, and industrial controls are safely separated from the outside world.



USE CASE

SHIPPING PORT OPERATOR

The steady flow of goods in and out of a country is of critical national importance and ports are a vital lifeline. If the port's network security is compromised, operations grind to a halt.

The Cybereason solution replaced a legacy installation that lacked the visibility that administrators needed to quickly identify and remediate threats. Cybereason On-Prem protects the port's servers and workstations with an Endpoint Detection and Response (EDR) and Next-Generation Antivirus (NGAV)/Endpoint Protection (EPP) combination that works together to automatically identify and sequester threats.

USE CASE

ENERGY PRODUCTION COMPANY

Providing 25% of a country's electricity needs, this company's data needs to be secure and isolated from the public Internet.

After testing all available on-premise EDR and EPP solutions, only Cybereason On-Prem was able to deliver greater network threat visibility and superior on-premise detection. Now the company can remain compliant with local regulations and safeguard their critical operations.

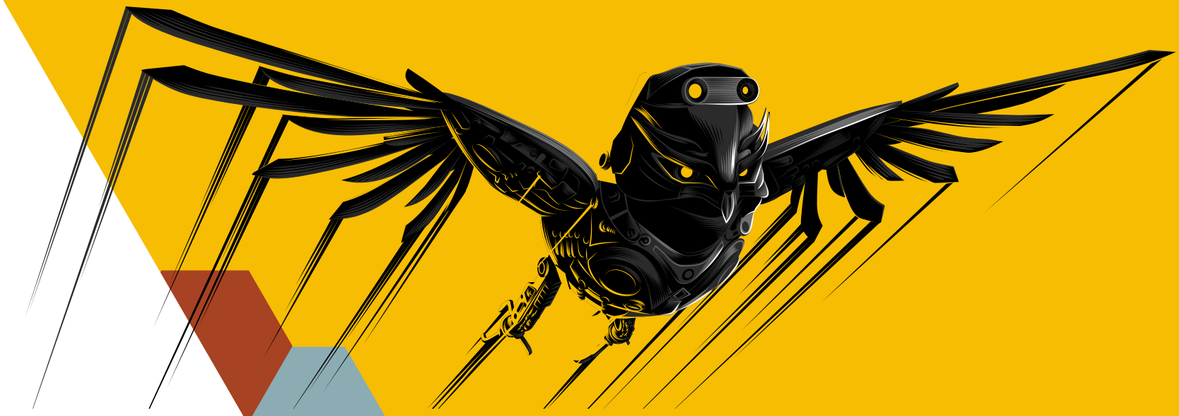
USE CASE

TRUSTED BANKING INSTITUTION

Strict data residency requirements and the sensitive nature of the organization's data called for an approach that could not be met by other solutions.

Cybereason On-Prem resolved security issues the bank didn't know they had with a broader detection capability than other solutions. Using machine learning and AI tools, Cybereason identifies threats without needing a connection to the Internet, which is crucial in the countries where this bank does business.

Cybereason On-Prem: no-connection protection



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.

Cybereason 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.

ON-PREM PEER REVIEWED

How Gartner's Peer Community rates the advantages of on-premises computing.

40%

say on-premises computing can offer businesses **more control** over their data and applications.

34%

say on-premises computing can be **more reliable** than cloud computing, since data is stored onsite.

13%

say on-premises computing can be more reliable than cloud computing, since it is **not subject to outages.**

11%

say **all** of the above.

Source: Gartner Peer Community poll.

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

Learn all about our **On-Prem** solution and access further information here.

Discover More

cybereason©

Cybereason is a privately-held international company, majority funded by Softbank and Softbank Vision Fund, headquartered in San Diego, California USA.

LEARN MORE AT CYBEREASON.COM