Technology in Europe

Protection without compromise for critical systems

European industry needs state-of-the-art solutions for maximum uptime.

cybereason

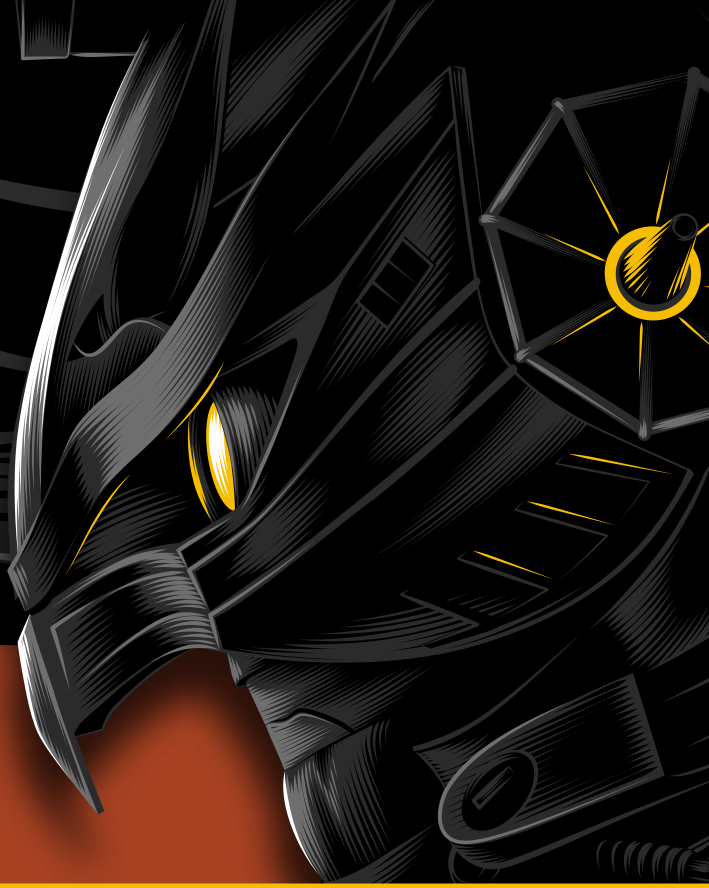
Introduction

Typical endpoint solutions require connections to the internet to receive updates and definition files, but vital infrastructure simply isn't allowed to connect to the internet.

Government guidelines introduced to safeguard consumer data and protect critical infrastructure are defining where **privileged consumer** and **operational data is stored.**

In this document, you'll see how three European organizations are protecting their operations to ensure maximum uptime with the only effective security solution for private networks 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 regulatory challenges facing industry leaders as they strive to protect privileged information using Cybereason's state-of-the-art tools.

Technology challenges for critical services

High availability isn't a luxury for critical infrastructure across Europe, it's mandatory. Key systems simply must work all the time despite changes in the weather, equipment failure, or the whims of a cybercriminal.

Under the watchful eye of regulators, organizations that provide critical services have the additional burden of keeping those services available and running smoothly while thwarting network intrusion.

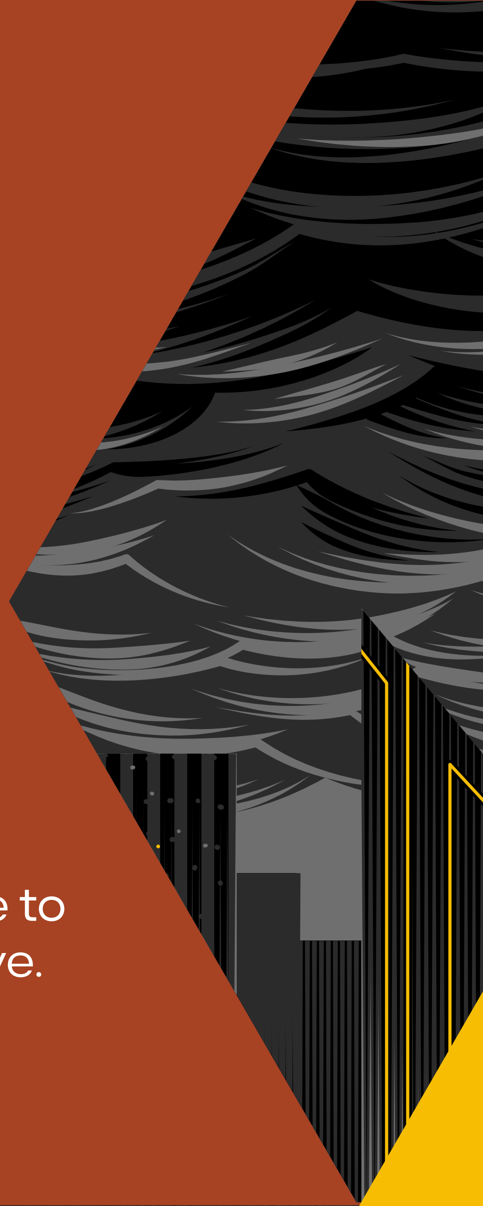
Critical industries across Europe need to take a strategic approach to protection. These solutions were designed specifically for their unique challenges to preserve uninterrupted operation and deliver superior resiliency.

USE CASE

NATIONAL ENERGY PROVIDER

Meeting the energy needs of an entire country requires that critical systems are always running, and beyond the reach of online attacks. As an essential service, the regulations are clear: they need to ensure resiliency in the event of a cyberattack, document any intrusions, and protect power delivery systems.

They provide a critical service, so their power generation and delivery networks are air-gapped from their public network connected to the internet. But these systems must still be managed and updated, leaving the infrastructure vulnerable to malware-induced sabotage from a single infected USB drive. They needed a solution to protect their private network without the need for an internet connection.



▶ Cybereason On-Prem offered the only on-premises solution that keeps data on the perimeter for both fully and partially air-gapped infrastructures.

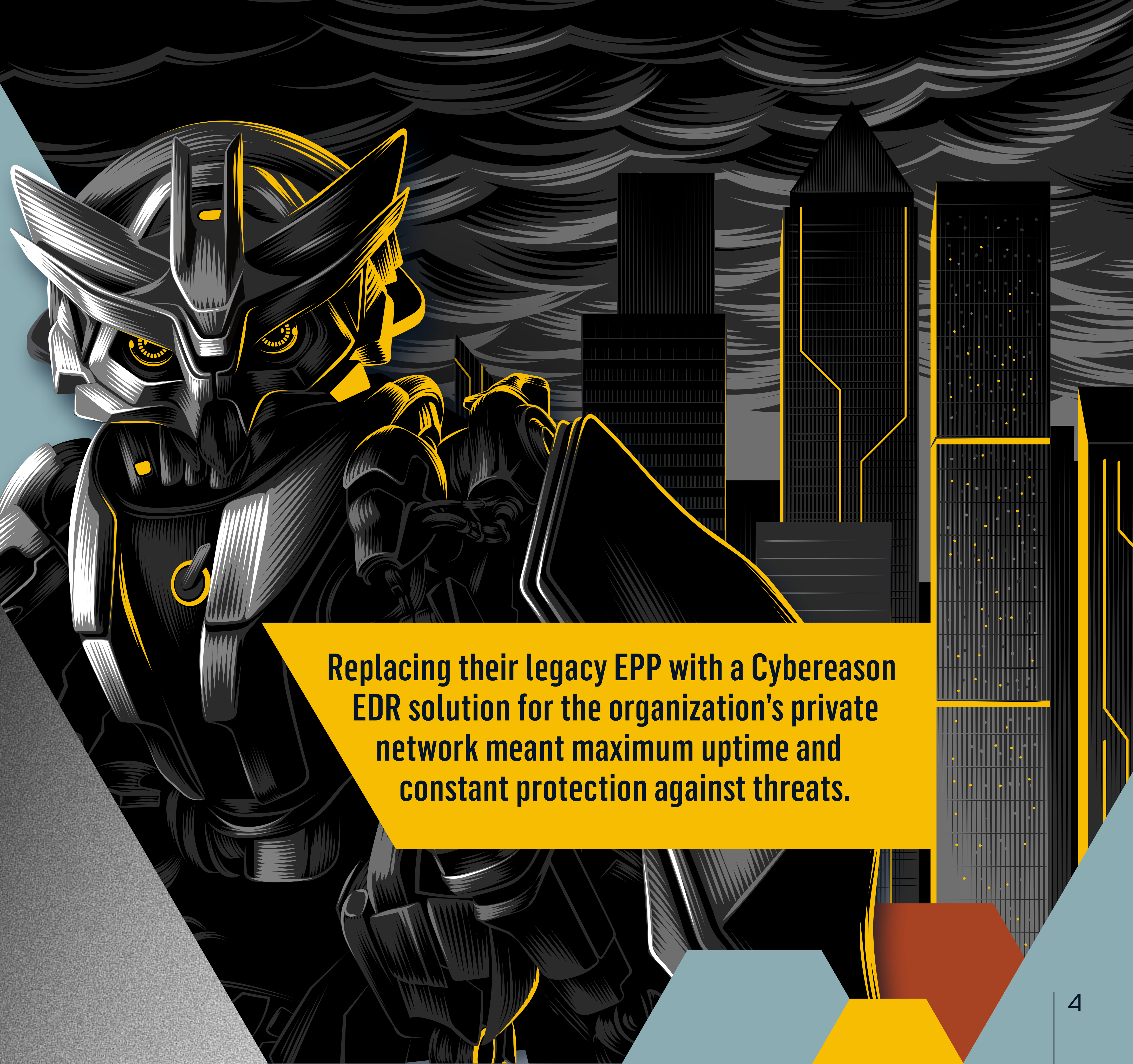
It uses Machine Learning and Artificial Intelligence to recognize abnormal behavior on the network. Once discovered, threats are neutralized, stopped from spreading, and mitigation efforts begin—often without operator intervention.

USE CASE

INSURANCE INDUSTRY LEADER

Customers share their most personal information with their insurance company and expect a response during the most stressful and harrowing times of their lives. Maintaining network security, even when an internet connection isn't available for updated virus definitions and software updates, led this insurer to choose Cybereason.

- Cybereason On-Prem was the only solution that allowed the organization to keep their critical information protected with a single, class-leading Endpoint Protection (EPP) and Endpoint Detection and Response (EDR) solution, even when disconnected from the internet throughout.



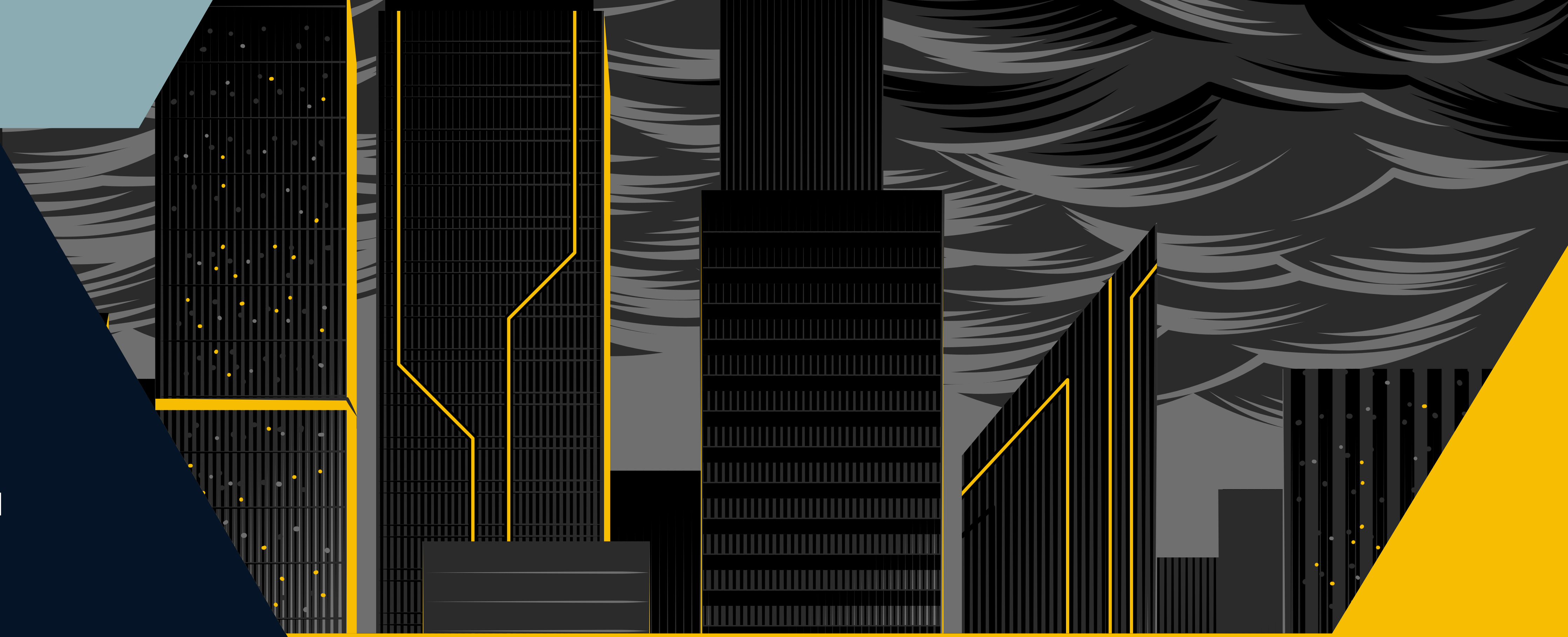
Replacing their legacy EPP with a Cybereason EDR solution for the organization's private network meant maximum uptime and constant protection against threats.

USE CASE

PRIVILEGED INFORMATION BROKER

This organization provides services to modernize the collection and dissemination of personal identity information. But when they needed to modernize their own outdated EPP, they chose Cybereason.

Allowing cybercriminals even a glance at the personal data they store would betray decades of trust and goodwill. Any EDR solution would have to identify and stop threats proactively.



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

Machine Learning allows vulnerabilities to be proactively identified and sequestered in minutes. The path any attack takes in the network is presented in a single, easy-to-understand console, with the threats identified for swift action and documented for regulatory compliance.

▶ **Cybereason's AI-powered EDR solution protects endpoints by recognizing malicious behavior on the network and stopping it before it spreads.**

The cybereason advantage

Whether your data is on-premise, in the private or public cloud, or a combination, Cybereason has the solution to keep cybercriminals out of your vital data.

PROTECTION

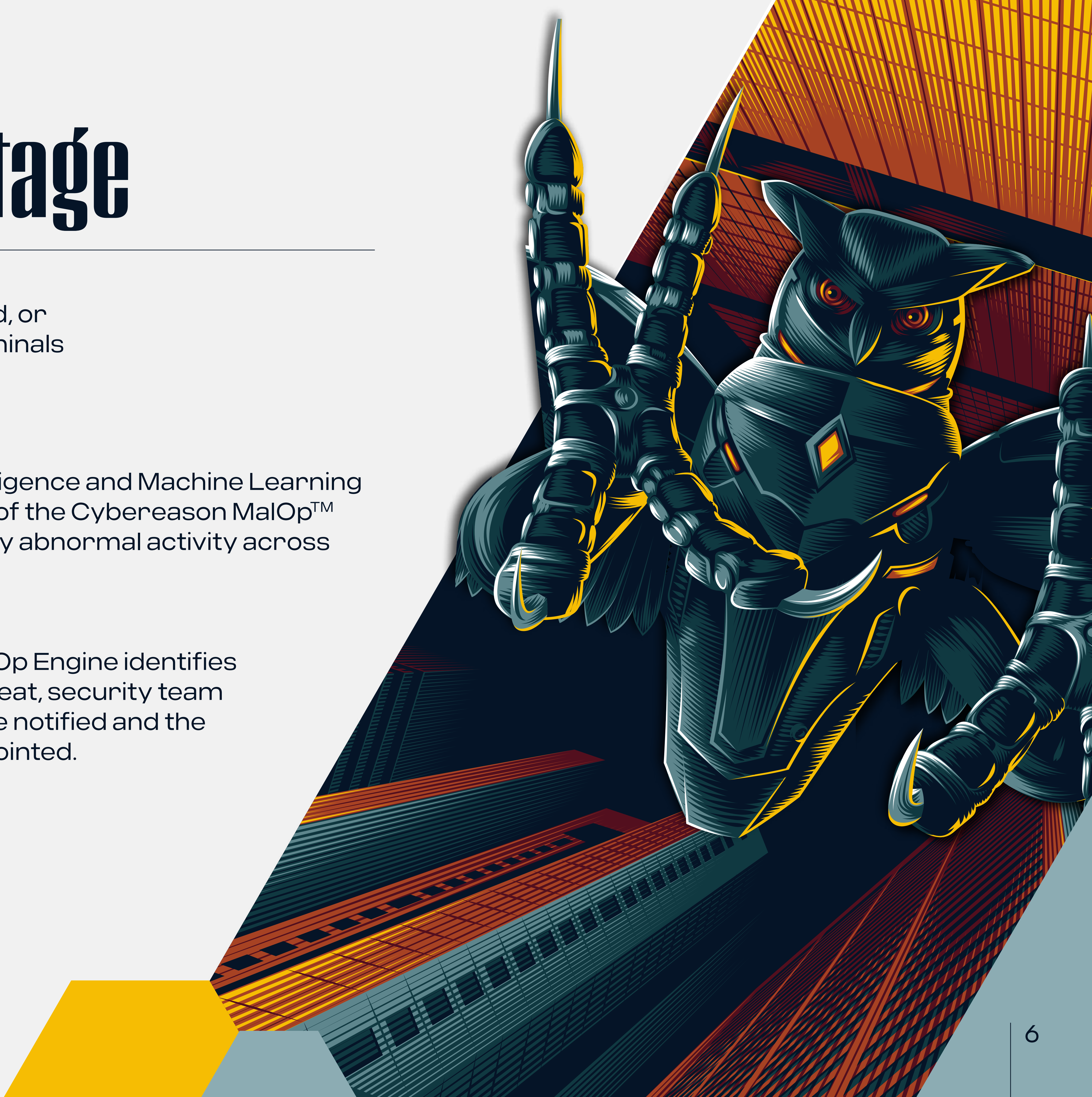
Cybereason is the only security vendor that delivers multi-layered NGAV prevention, where each layer is purpose-built to prevent unique attacker techniques. Cybereason provides unparalleled attack protection by combining 9 independent yet complementary prevention layers, ensuring that your business achieves its goals and bad actors don't.

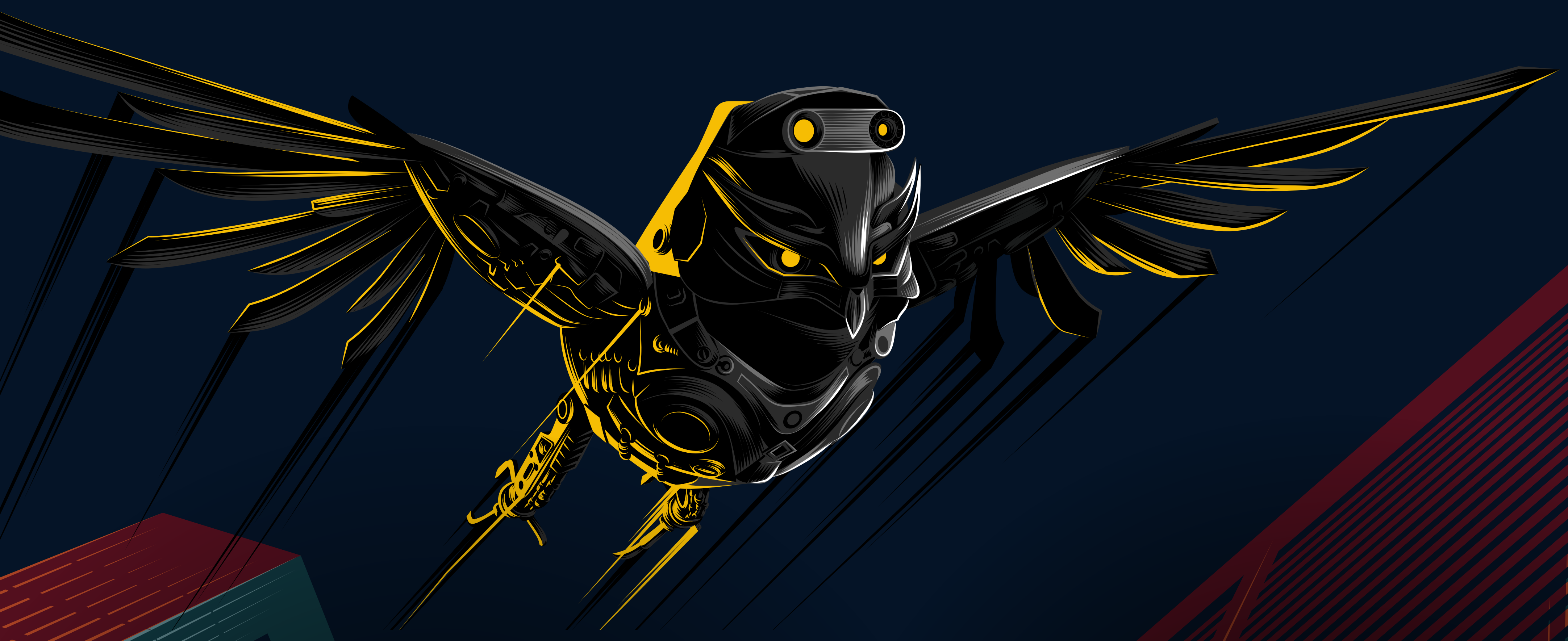
DETECTION

Artificial Intelligence and Machine Learning components of the Cybereason MalOp™ Engine identify abnormal activity across the network.

INVESTIGATION

Once the MalOp Engine identifies a possible threat, security team operators are notified and the threat is pinpointed.





DOCUMENTATION

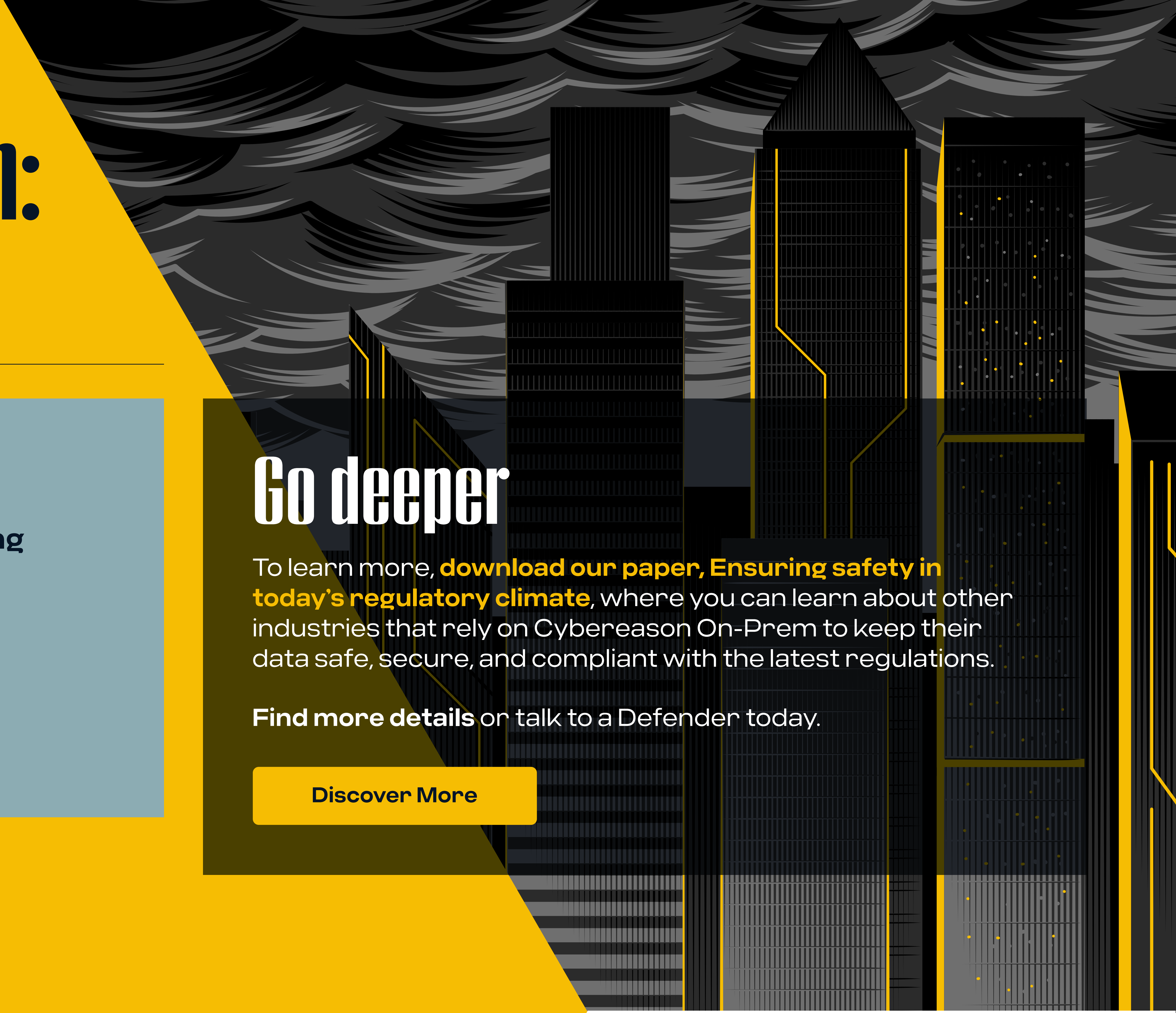
The security team receives a map of what has happened, who is affected, and any remediation steps needed. Cybereason also provides the only platform on the market that reveals the complete history of an attack automatically, in real-time.

REMEDIATION

The MalOp™ sees the full picture of the attack. We then take it a step further and populate tailored response playbooks that remediate the complete intrusion in one fell swoop. With Cybereason, Defenders can orchestrate and automate response to all impacted users and endpoints with a single click. This automation means reduced MTTR and extra bandwidth for security analysts.

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, Ensuring safety in today's regulatory climate**, 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©