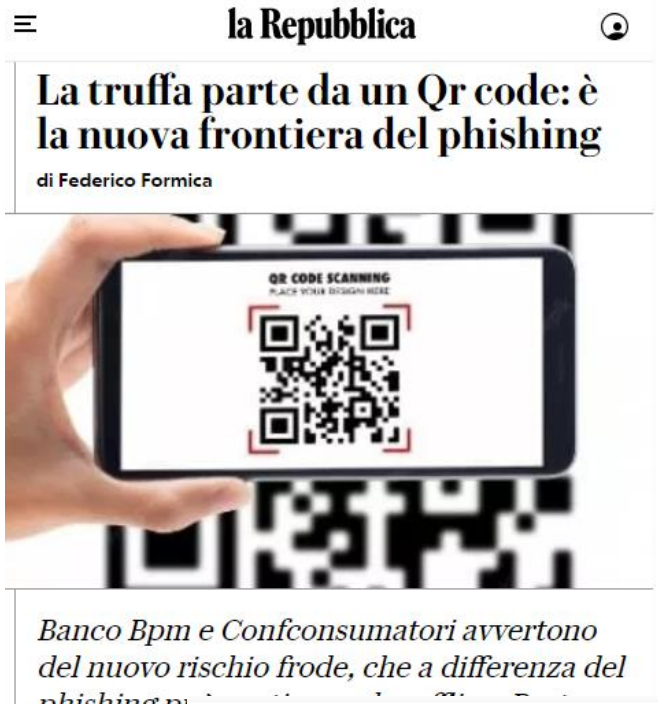
mobisec

WINNERS PLAY IT RIGHT

# 360° Cybersecurity

**Mobisec LLC**
440 N Wolfe Rd.
Sunnyvale, CA 94085

**Mobisec Italia Srl**
Viale della Repubblica 22
31020, Villorba (TV)



la Repubblica

## La truffa parte da un Qr code: è la nuova frontiera del phishing

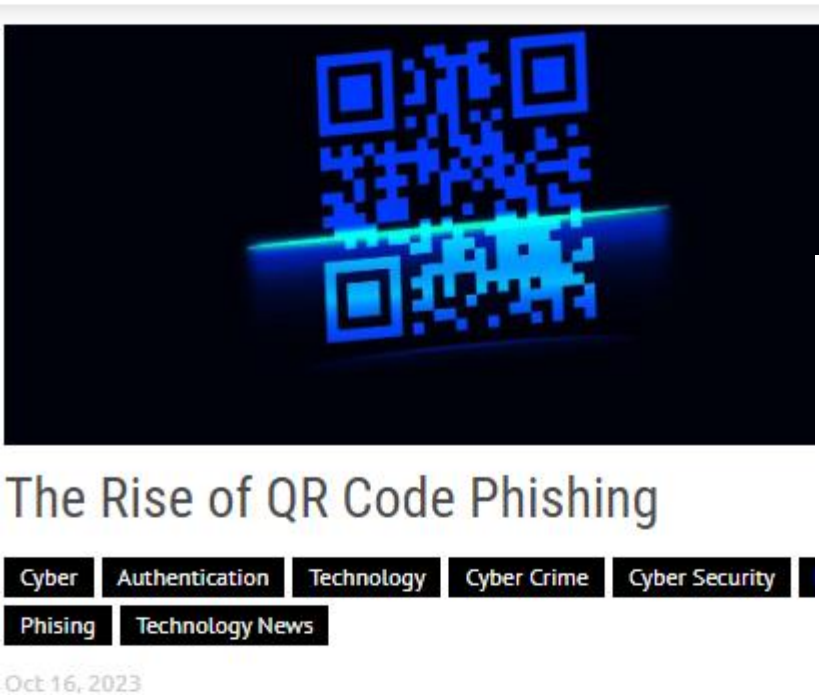
di Federico Formica

*Banco Bpm e Confconsumatori avvertono del nuovo rischio frode, che a differenza del phishing p*

*volantino o*

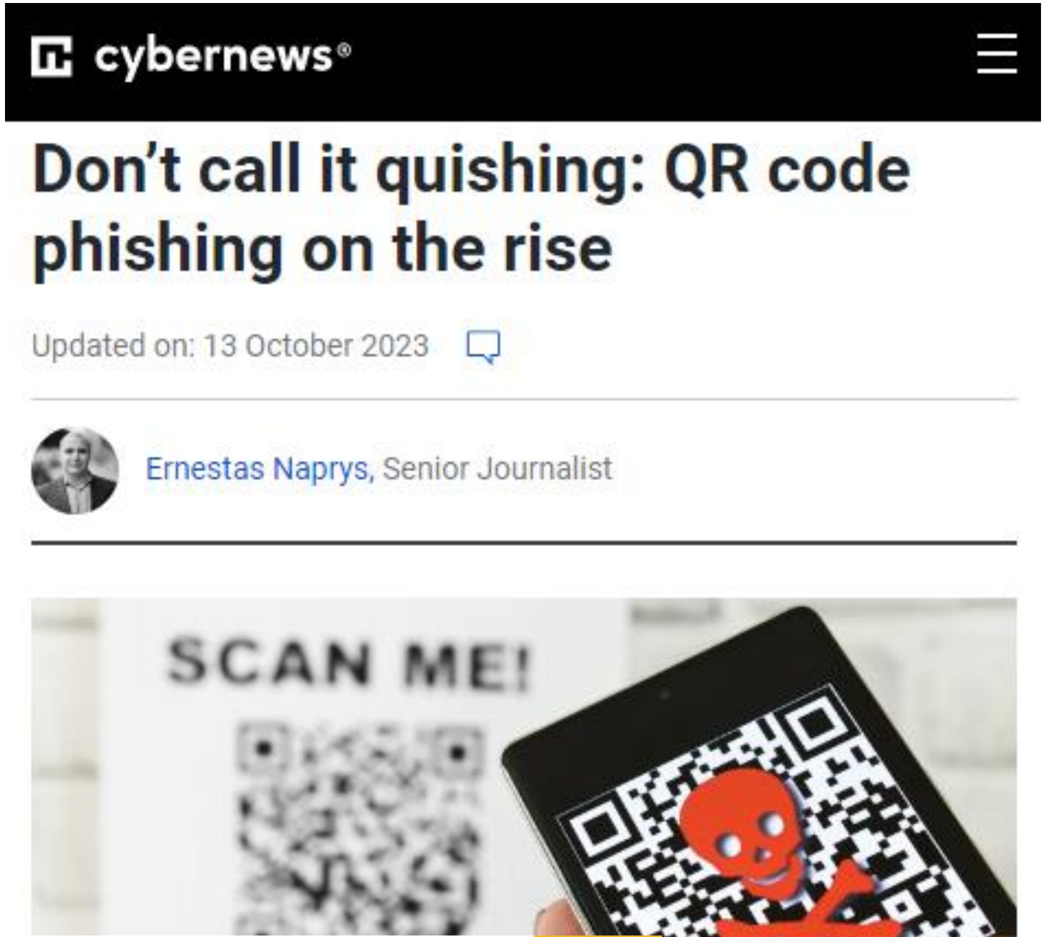
*all'interno*

06 NOVEMBRE 202



## The Rise of QR Code Phishing

Oct 16, 2023



cybernews®

## Don't call it quishing: QR code phishing on the rise

Updated on: 13 October 2023

Ernestas Naprys, Senior Journalist

BANCO BPM

## QRishing: la truffa del QR Code.

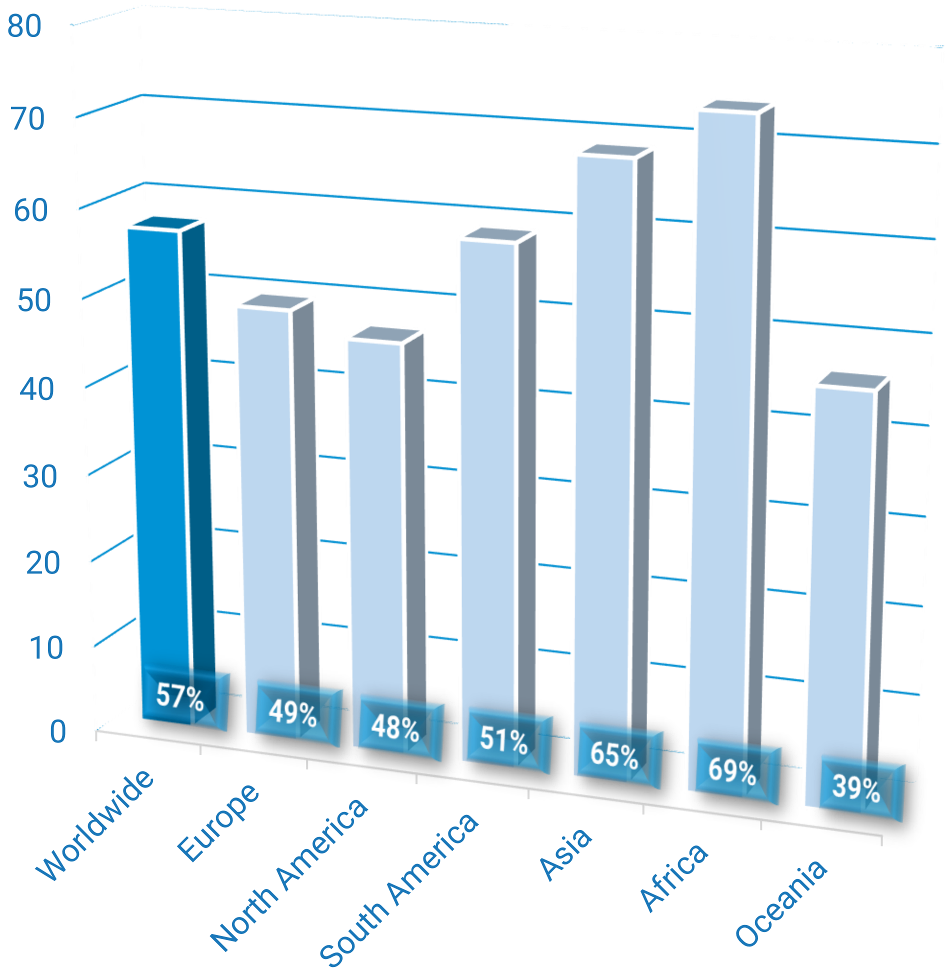
mobisec

# Data & Facts

# A new Scenario

A quick glance at the mobile world

Today, **more than half of the world's population** surfs the Web from mobile devices.



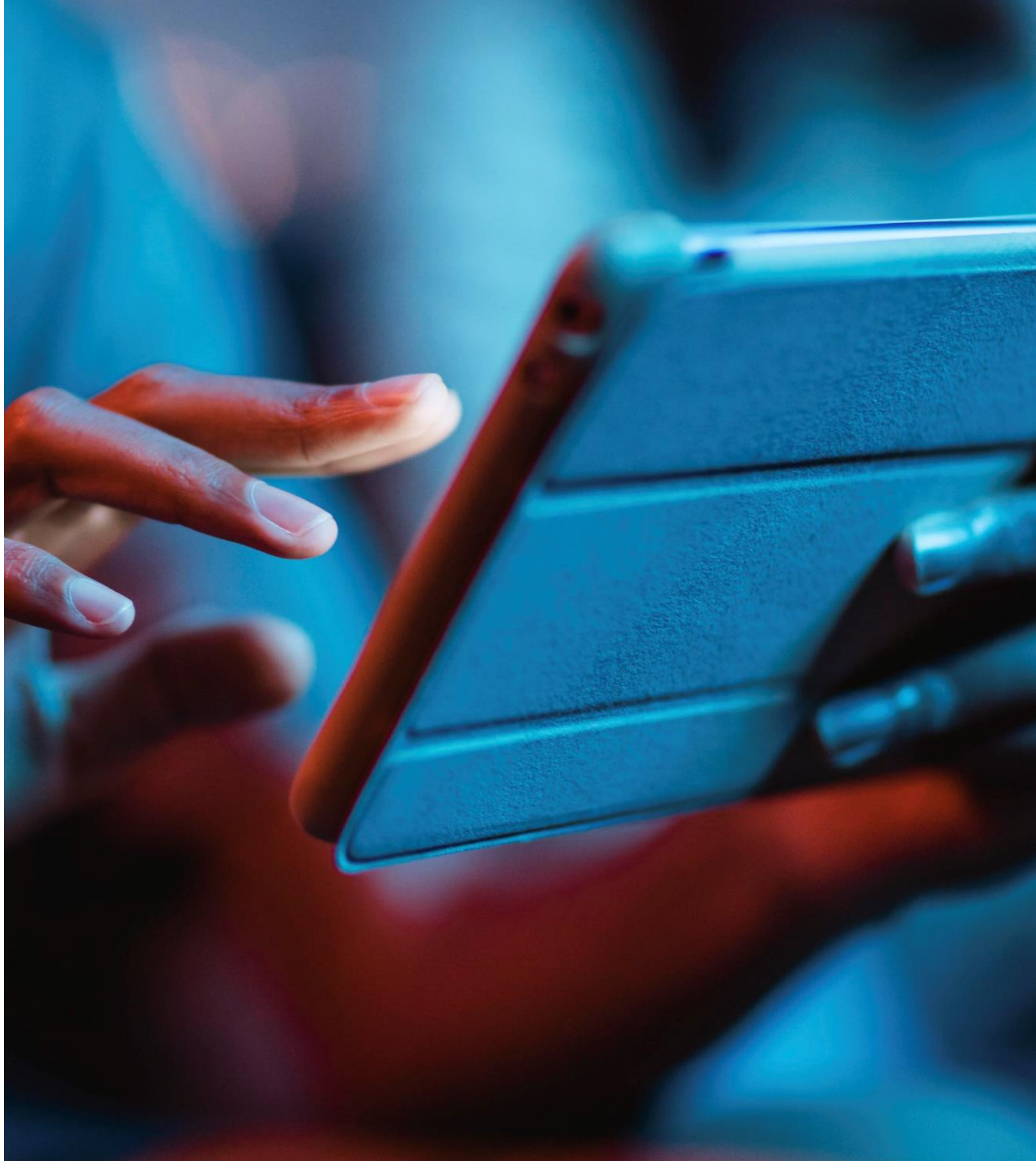
Source: Internet Traffic from Mobile Devices (Aug 2023) (explodingtopics.com)

Mobile devices today are an essential part of our lives, from communicating with loved ones to managing business on the go.

**However, there is the flipside of this technology: cyber attacks.**

Cyber criminals are constantly looking for vulnerabilities not only in mobile devices, but mostly in applications, which lead, if exploited, to **potentially devastating consequences such as data breaches and financial losses.**

**In today's interconnected world, it is more important than ever to secure devices and applications.**



mobisec

You may never know if the app,
the device or the website
you are using
are vulnerable or not.

**Hackers do.**

mobisec

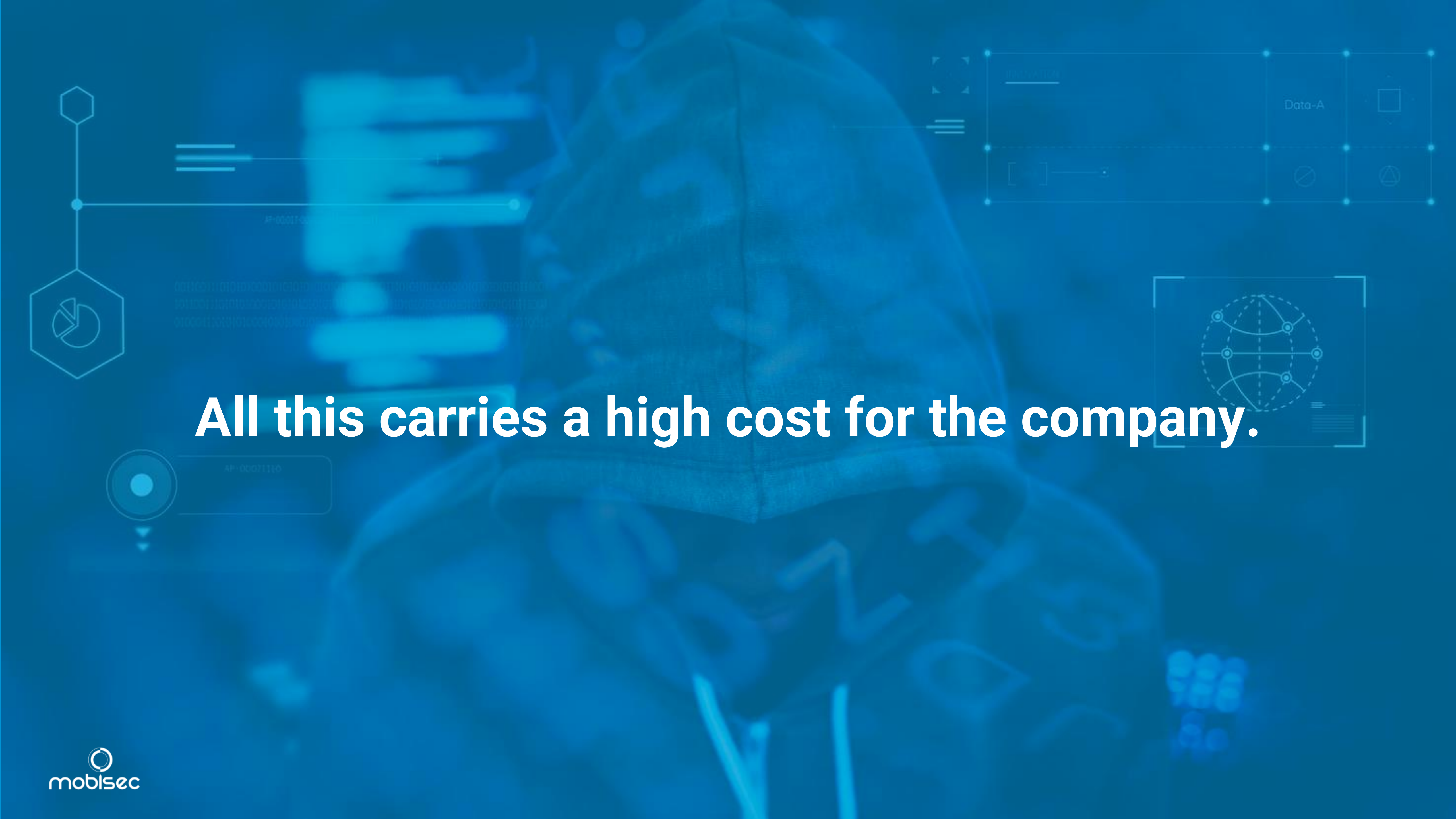
# Welcome to the jungle

## what dangers you are running into

**Once a malicious attack occurs successfully, it is easy to gain access to:**

- **Confidential information**
- **Users' personal and sensitive data**
- **Customer behaviors and profiling**
- **Corporate know-how**
- **Can compromise economic transactions**

*And much more...*



# All this carries a high cost for the company.

# $9.44 Millions

This is the average damage caused by a data breach in the US.

The total damage for the **year 2025** is expected to **exceed $10.5 trillion globally.**

Source: Cost of a Data Breach Report 2022 (IBM)

**60%** of breaches suffered lead to increased costs to customers

**19%** of breaches are caused by downward service agreements negotiated with vendors

**83%** of companies experienced more than one data breach

Source: Cost of a Data Breach Report 2022 (IBM)

# A new Scenario

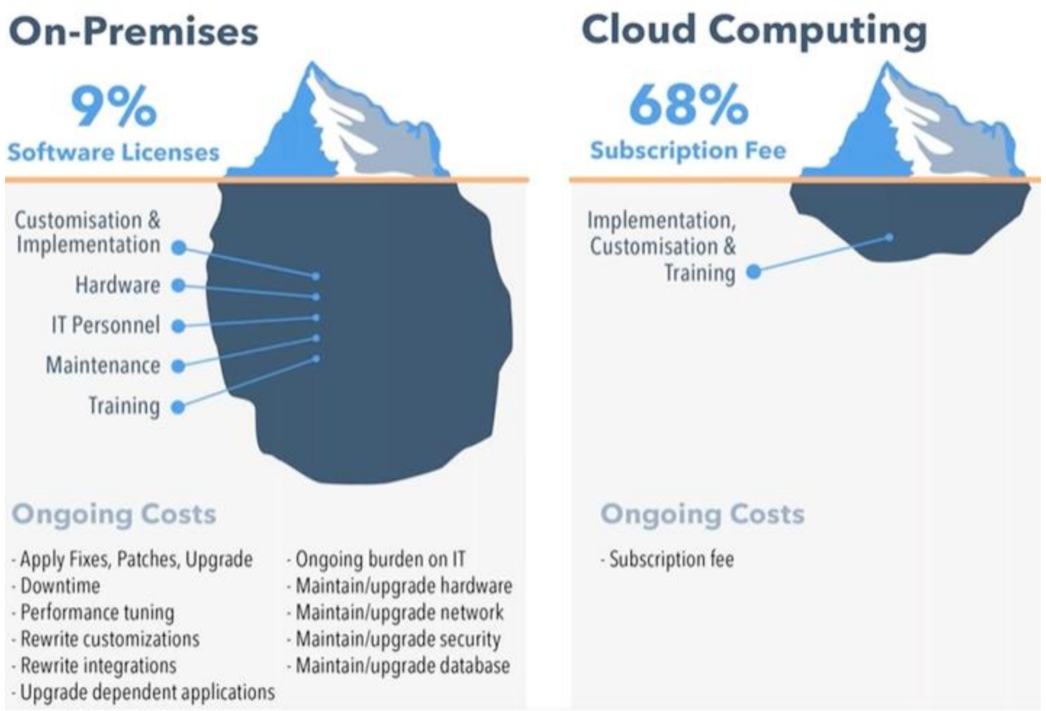
When it comes to cyber security, current budget allocations heavily favour network and infrastructure security (51.6%) over application security (2.4%).
Most organisations are investing heavily in securing their network and infrastructure.

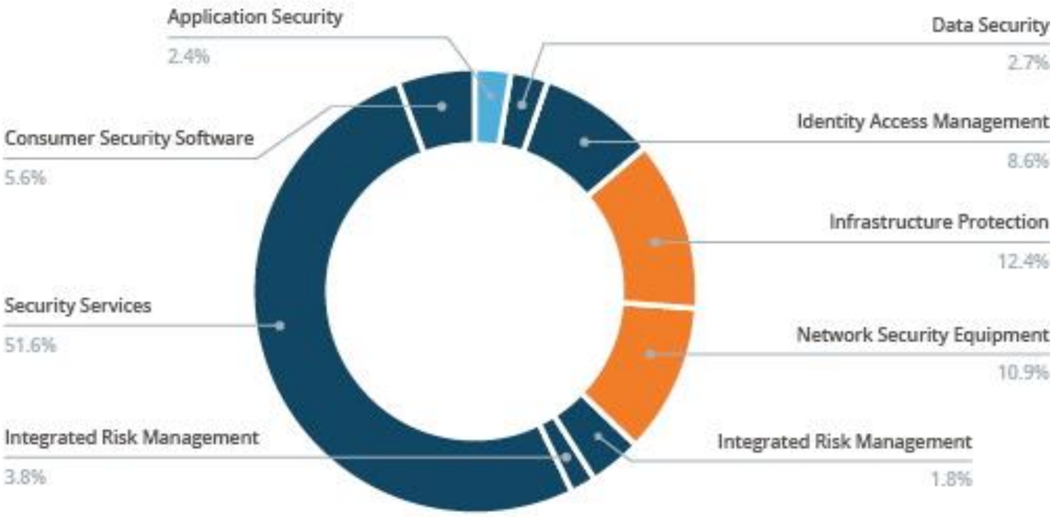
**However, a significant shift is underway.**

Over the past 5 years, organisations large and small have been moving from in-house / on-premises solutions to cloud-based alternatives.

This shift is reshaping the cybersecurity landscape.

Until recently, the network and infrastructure were the most vulnerable and cost-effective targets for cyberattacks.





# Who is mobisec ?

# Mobisec

## Birth and growth of a unique cyber firm

- **Founded in 2015** with a focus on **mobile cybersecurity**
- **Industry pioneers in Europe** for 8 years, working with leading, technologically advanced clients
- Our innovative approach consistently delivers **superior value recognized by the market**

# Who trusted us?

flowe

AUTOGRILL

ADR Aeroporti di Roma

GENERALI

AMMAN

ING

sara

FINECO BANK

Carrefour

Ministero della Salute

Regione Lombardia

LEROY MERLIN

REGIONE TOSCANA

sogei

AXA

F1™

LEONARDO

BNL GRUPPO BNP PARIBAS

City of Westminster

Allianz

Telepass

ESSELUNGA

MEF Ministero dell'Economia e delle Finanze

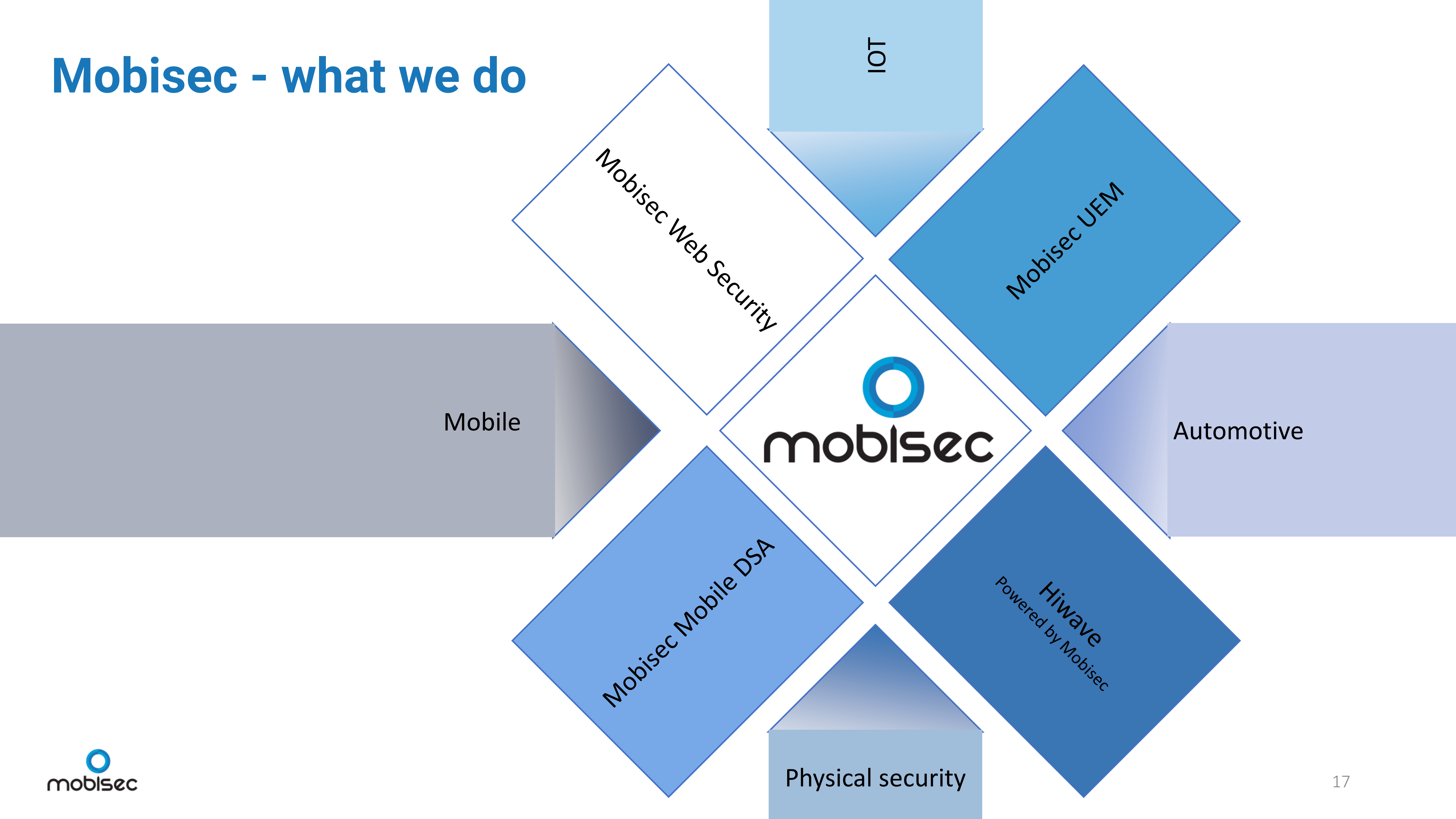
UniCredit

And others…

mobisec

# What we do

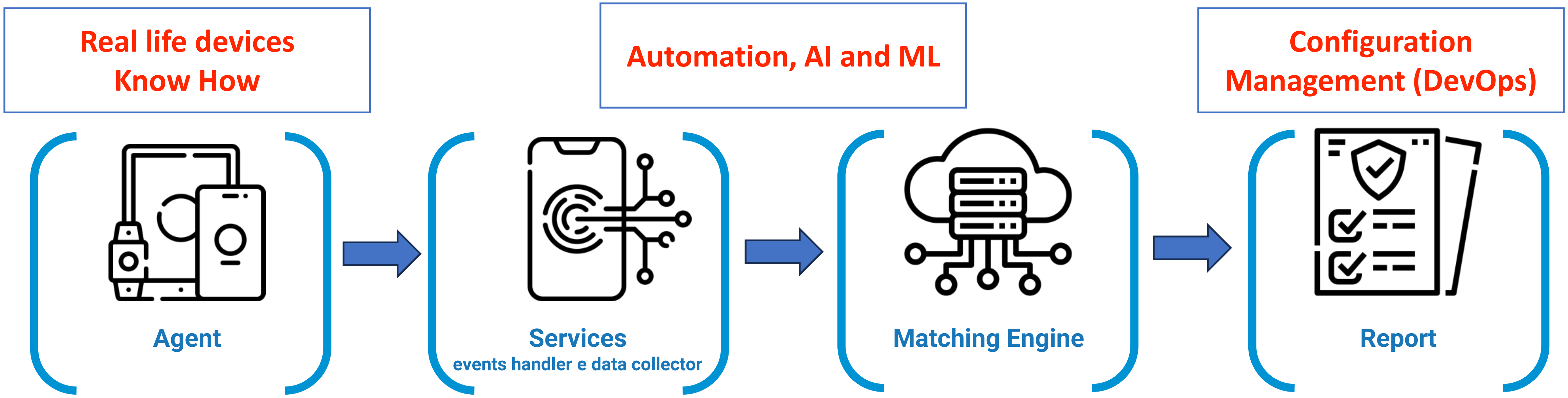
# Mobisec - what we do



# Mobisec Dynamic Security Analysis

## How it's made.

Mobisec DSA is a platform structured on 4 main components:



Real life devices Know How

Automation, AI and ML

Configuration Management (DevOps)

Agent

Services
events handler e data collector

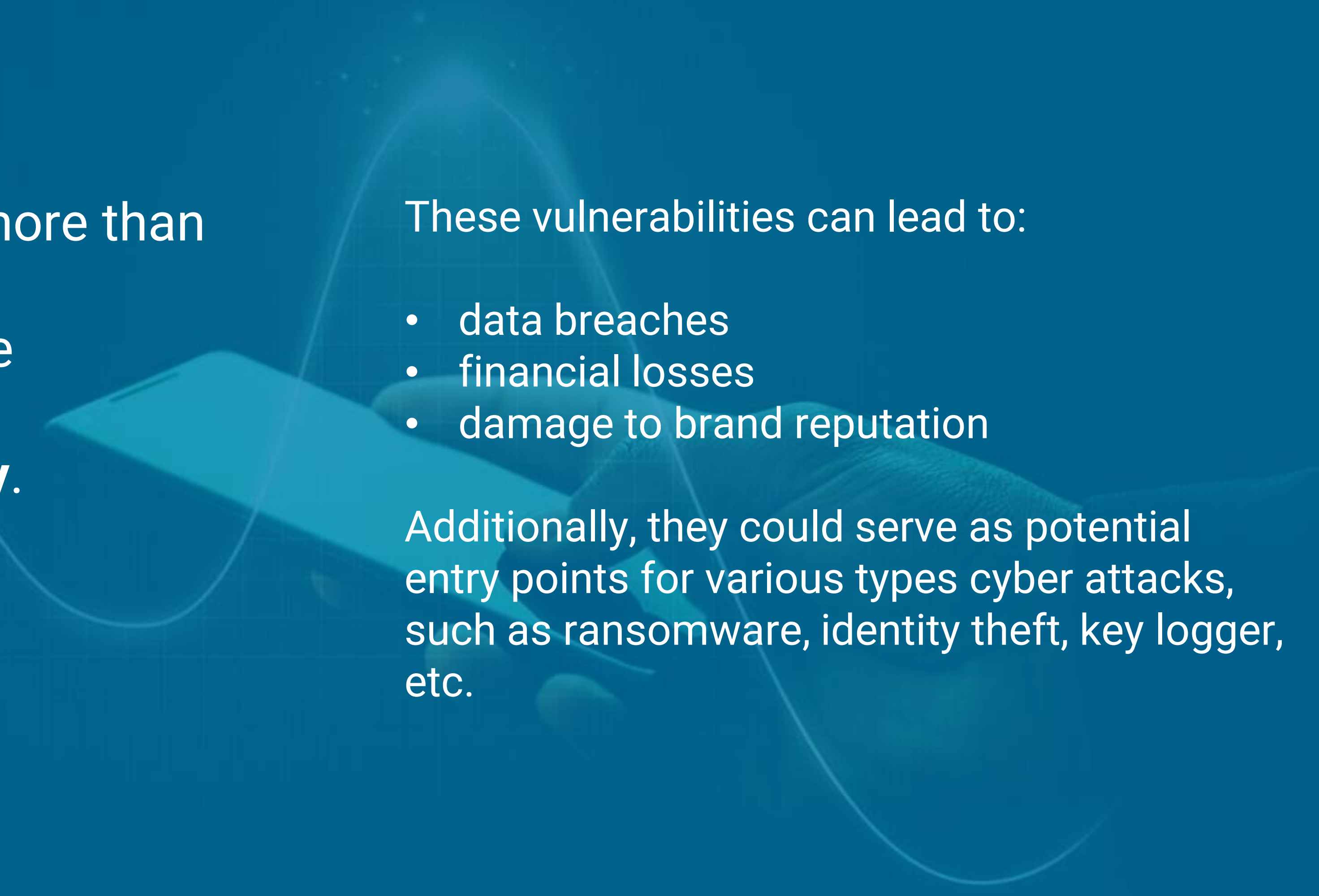
Matching Engine

Report

Each component interacts with the application, its functions, processes and the data generated by using it.

# Mobisec Dynamic Security Analysis

## Our learning by experience



In more than **8 years** we conducted more than **10.000 mobile application analysis**. We discovered that **98%** of the mobile applications that had been tested had **at least one** security **vulnerability**.

**Out of these, 70% had high-risk vulnerabilities*.**

*Standard CVSS > 7.0

These vulnerabilities can lead to:

- data breaches
- financial losses
- damage to brand reputation

Additionally, they could serve as potential entry points for various types cyber attacks, such as ransomware, identity theft, key logger, etc.

# Mobisec DSA

## How does it work?

Mobisec's Dynamic Security Analysis **examines the development logic of the app** as well as its security by testing it on actual devices **in our laboratory**.

Unlike other cybersecurity companies that mostly concentrate on network security and rely on emulators, **Mobisec DSA detects vulnerabilities by analyzing the actual functioning of devices.**

**It identifies weaknesses that would remain hidden if static or emulator-based assessments were conducted**.

## OUR COMPETITORS

mobisec

# Mobisec DSA

## A case study

### Overview

Mobisec began working with an international bank in 2017.
Focused on evaluating the safety of the Italian banking app and ensuring adherence to group guidelines.

### Key Points:

Established a closer partnership with key stakeholders: Product Owner, Project Managers, and lead developers.
Aimed to improve app development and address security vulnerabilities exploited by attackers.

### Challenge:

Address the growing threat of malware attacks targeting the bank app on Android systems.
Aspire to make the Italian bank app the most secure among the group's branches.

### Results:

Following Mobisec's strict guidelines led to a significant reduction in malware attacks over the past few years.
The Italian bank app now serves as a security model for banking apps within the Group.
Enhanced security safeguards customer data, builds trust, and contributes to the ongoing success of the Italian branch.

# Mobisec DSA in brief

- Analyses native, hybrid and API gateway applications
- Performs static and dynamic analysis
- Vulnerability testing from design to provisioning
- Integrates with your organization's configuration management systems
- Apps are tested in a real-world usage context
- Checks every app data, function, transaction and component
- First full report in 5 days, for subsequent testing in just 2 days

mobisec

# services

# VAPT/WAPT

## Test and assess the actual

Vulnerability Assessment and Penetration Testing (VAPT) are two key components of cyber security:

- **Vulnerability Assessment** (VA) aims to identify known issues to prevent common industry mistakes.

- **Penetration Testing** (PT); also known as **Web Application Penetration Testing** (WAPT), conducts a thorough examination of code, algorithms and logic to uncover potential vulnerabilities such as data leakage, account takeover and privilege escalation.

**WAPT follows the OWASP WSTG (Web Security Testing Guide) best practices**, which cover a wide range of scenarios to identify vulnerabilities at different levels.

# Common Vulnerabilities and Exposures MONITORING

## Keep it safe in its lifecycle

Throughout the software development lifecycle, we maintain **a 24/7 service that collects data from the CVE and CWE online databases.**

We compare this data with the libraries and plug-ins used in the project **to identify vulnerabilities and weaknesses.**

This information is shared with developers and project managers for timely **hot fixes and risk management**.

In addition, **our solution extends beyond development** to ensure ongoing middleware patches and security package updates through regular maintenance.

# Hiwave

## Data monitoring, measurement, management and security

With **Hiwave by Mobisec**, we help enterprises to secure, supervise and manage IoT devices, apps, users and data **directly into enterprise systems and devices.**

Mobisec Hiwave can be **integrated into any device** and can provide **continuous supervision and direct control over**:

- Acquisition and normalization of big data from any device
- Technical troubleshooting
- Anti-fraud
- Active and applied security
- Marketing profiling
- Business performance monitor
- Operational measurement
- Business continuity
- Predictive Analysis

# Mobisec Unified Endpoint Management Assessment

## Secure enterprise devices

Unified Endpoint Management (UEM) streamlines IT management, security, and deployment across all enterprise devices from a single console, addressing the challenges of securing and connecting diverse device environments, including remote work, IoT, and legacy system integration.

**To not manage correctly enterprise devices brings to:**

- **Inadequate solutions**
- **Device configuration errors**
- **Misuse of devices by employees**
- **Fraud attempts targeted at corporate mobile devices**

# App Scraping

**Mobile App Scraping is a tool that monitors alternative app markets using a proprietary engine developed by Mobisec.**

It operates **semi-automatically** on a keyword basis and has an accompanying human operator for monitoring.

Out there, there is a wide selection of app stores, as well as the official Google store. **These stores can be accessed on rooted or non-rooted devices.**

The following is an indicative and non-exhaustive list (which is regularly updated) of the primary market channels for Android applications:

- Google Play
- Huawey App Gallery
- Samsung Galaxy Store
- Amazon App Store
- Aptoide
- APKPure
- Uptodown

# Cybersecurity training

Mobisec provides innovative training programs for companies with the following features:

- **Practice First:** we use a reversed methodological approach, beginning with practical experience to immerse individuals in actual secure development scenarios from the outset.

- **"Screen and Match" Strategy:** at the start of the training, we capture the current state, enabling a "before-and-after" comparison of learning outcomes upon training completion.

- **Focus on Metrics:** we prioritize training that focuses on measurable results. Learn how to monitor secure development effectively using specific KPIs from the Metrics Manifesto.

Each participant can interact with a highly qualified mentors for one-to-one mentorship and gain a deep understanding of the topics discussed during the training.

**Our courses offer full remote learning flexibility.**

mobisec

# Market

# Market’s data

## a quick glance

## Global Mobile Security Market

2019 → 35$ billion
2027 → 104$ billion

(CAGR +19,4%)

(Global & Europe data - 2022, Fortune Business Insights)

# Market's data

## a quick glance

## European Mobile Security Market

2019 → 3$ billion
2027 → 12$ billion

(CAGR +19%)

(Global & Europe data - 2022, Fortune Business Insights)

# Market's data

## a quick glance

## Italian Cybersecurity Market

2022: 1.86€ billion

- **50% comprises cybersecurity solutions***
- **There has been a 23% growth in endpoint security**

*Endpoint and Extended Detection and Response, SIEM, Identity & Access Management, Vulnerability Management, and Penetration Testing

(Italian data - 2023, Osservatorio POLIMI)

# Market's data

## a quick glance

## Italian Market

- Italian cybersecurity companies are nearly 3,000 (+6.3% from 2019)
- 815 businesses are formed as limited companies

## Number of companies by Region

### First five rankings

| Ranking | Number | Region |
|---:|---:|---:|
| 1 | 679 | Latium |
| 2 | 535 | Lombardy |
| 3 | 304 | Campania |
| 4 | 207 | Sicily |
| 5 | 194 | Veneto |

(2021, Unioncamere)

# Competitors

# Some Competitors

| | | | |
|---|---|---|---|
| 🇮🇹 | UNLOCK SECURITY | CRYPTONET LABS<br>a DIGITAL360 company | SOTERITSECURITY<br>Beneath the surface, always<br>ARGO CYBER |
| 🇪🇺 | WITH secure | jscrambler | Acronis |
| 🌍 | VERACODE | CHECK POINT | HCLSoftware |

mobisec

# SWOT

**Helpful**

**Harmful**

**Internal Origin**

Strength

Strong expertise in mobile security

Innovative solutions

Customization

Strong client relationship

Weakness

Dependance on tech advancements

Resource Allocation

**External Origin**

Opportunity

Cybersec awareness

Data security concerns

International expansion

Growth in mobile and IoT

Threat

Market Competition

Rapid tech changes

mobisec

mobisec

# A challenge for you

# Chose Your challenge

- Market Research Challenge
- Communication Strategy Challenge

# Chose Your challenge

## Market Research Challenge:

**Objective**
Conduct in-depth market research in mobile / IoT cybersec sector

**Task**
Analyze market trends, prospects behavior and competitive landscape.

**Data Collection**
Gather data through surveys, interviews, and secondary research.

**Analysis**
Interpret findings to identify opportunities, challenges, and potential market gaps.

**Presentation**
Prepare a report in order to present findings

# Chose Your challenge

## Communication Strategy Challenge:

**Objective**

Develop a communication strategy for Mobisec.

**Task**

Create a compelling narrative and messaging plan.

**Audience Analysis**

Identify target audiences and their preferences.

**Channels**

Choose appropriate communication channels (e.g. social media, traditional advertising…)

**Budget**

Allocate a hypothetical budget to maximize impact.

**Presentation**

Prepare a report in order to present the strategy

***“When you do things right, no one will suspect that you actually did anything.”***

*- Futurama -*

# Thank you

**Mobisec LLC**
440 N Wolfe Rd.
Sunnyvale, CA 94085

**Mobisec Italia Srl**
Viale della Repubblica 22b
31020, Villorba (TV)
+39 0422 1784435

# Glossary

**CVE** - is a list of publicly disclosed computer security flaws. When someone refers to a CVE, they mean a security flaw that's been assigned a CVE ID number. CVEs help IT professionals coordinate their efforts to prioritize and address these vulnerabilities to make IT systems more secure.

**CVSS** - Common Vulnerability Scoring System. It's a way to evaluate and rank reported vulnerabilities in a standardized and repeatable way. The goal of CVSS is to help you compare vulnerabilities in different applications – and from different vendors - in a standardized, repeatable, vendor agnostic approach. CVSS generates a score from 0 to 10 based on the severity of the vulnerability. By using CVSS to prioritize vulnerabilities, companies can focus on the most critical ones first and reduce the overall risk to organizations.

**IoT** - Internet of Things refers to the interconnectedness of physical devices, such as machinery, home appliances and vehicles, that are embedded with software, sensors, and connectivity which enables these objects to connect and exchange data. This technology allows for the collection and sharing of data from a vast network of devices, creating opportunities for more efficient and automated systems.

**Rooted device** - rooting is the process of unlocking an Android device to gain administrative control, similar to jailbreaking. It provides access to Android subsystems, circumventing restrictions. Rooted devices can install unapproved apps, modify the system, and customize settings. It also allows for installing Custom ROMs, offering extensive customization for Android users.

**VAPT** - Vulnerability Assessment Penetration Testing aims to identify known issues to prevent common industry mistakes.

**WAPT** - Web Application Penetration Testing, conducts a thorough examination of code, algorithms and logic of web applications to uncover potential vulnerabilities such as data leakage, account takeover and privilege escalation.

**Web Application** - is any computer program that performs a specific function by using a web browser as its client. The application can be as simple as a contact form on a website, or it can be as complex as a multi-player mobile gaming.