



# CELTIC-NEXT Launch Event



9<sup>th</sup> of December 2022, Online via WebEx

Pitch of the Project Proposal

## European Mobile Cyber Protection

**Acronis**

**Presenter:** Plamen Toshev,  
Head of Acronis Mobile, Managing Director Acronis Bulgaria

**Contact:** [vlad.dv@acronis.com](mailto:vlad.dv@acronis.com)

# European Mobile Cyber Protection - Aim



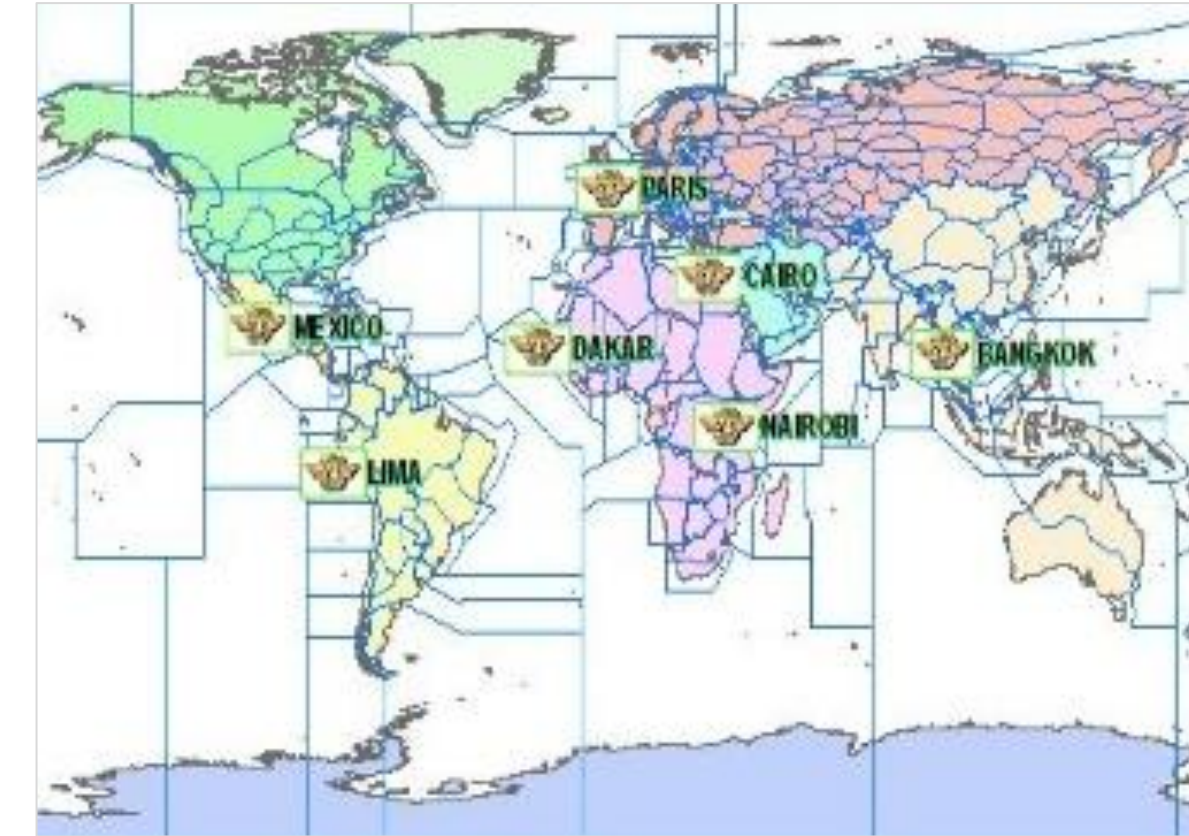
Protect IoT and mobile devices from modern cybersecurity risks like:

phishing and grayware

while ensuring European sovereignty over data



# Acronis - Company profile



Dual Headquarters for Dual Protection

**Acronis** is Cyber Security company which protects the data, applications, systems and productivity safeguarding them against cyberattacks, hardware failures, natural disasters and human errors.

- Since **2008** Corporate HQ in Schaffhausen, Switzerland

- Founded in **2003** in Singapore, currently the International HQ

## Global Local Presence

- 2,000+** employees
- 34+** R&D locations
- 150+** countries
- 26+** languages
- 49** data centers

Acronis aims on innovative development of its machine-intelligence powered **Cyber Cloud, Cyber Protection, Cyber Platform**



# European Mobile Cyber Protection - Problem Statement



## 1. Phishing is on the rise

- 2020: Mobile **phishing** ↑ **300%** (Proofpoint)
- 2021: **75x** more **phishing** websites than malware websites with 2,145,013 websites registered by Google (**27%** increase over the last 12 months)
- 2021 – 2022: Mobile is the preferred platform for reading emails (Gartner Mobile Threat Defense Market Guide)

## 2. Grayware apps, privacy

- **742** apps published per day in AppStore, **3,739** apps published per day in Google Play (AppInventiv, 42 matters)
- **62%** of employees at small and medium businesses use smartphones for work purposes, compared to 64% in enterprises (IDC's 2019 Enterprise and SMB Mobility survey)

## 3. European data sovereignty

- Main mobile platform vendors are non-European
- Mobile device data is stored in DCs outside of Europe
- Controls for security and privacy in apps is in the hands of multiple vendors

# European Mobile Cyber Protection – Gaps & Solutions



Gap

1. Phishing is on the rise

Solution

- **Phishing Prevention:** Protect online behavior by preventing opening of malicious websites on the mobile device
- **Antimalware**
- **Virtual Private Network (VPN)**
- **Network Security**

Gap

2. Grayware apps, privacy

Solution

- **App vetting:** Machine learning-based cloud protection from **grayware** apps
- **Mobile device management**
- **Data Leakage Detection**

Gap

3. European data sovereignty

Solution

- **Cloud mobile Backup and Restore**
- **Store device data in European cloud datacenters**
- **Device Compliance**

- **Built-in solution into device (via Partnership with Telecoms)**

# European Mobile Cyber Protection - Details



Feature/Solution	Description/Value	Participants	Competences
App Vetting	Machine-learning based feature that can identify <b>grayware</b> apps, preventing deployment on the customer mobile devices.	<ul style="list-style-type: none"> <li>Acronis</li> </ul>	V
IoT and Mobile Device Management	Prevents unsafe user's behavior by utilizing device and application policies. Enables remote lock and wipe. Provide device reputation and zero-trust access capabilities.	<ul style="list-style-type: none"> <li>Partner-Vendor</li> </ul>	Existing solution
Mobile Backup and Restore	Protects customers' mobile device data, contacts, messengers data and media content in local or hybrid encrypted storages.	<ul style="list-style-type: none"> <li>Acronis</li> </ul>	V
Antimalware	Provide malware protection on all types of workloads, including IoT and mobile. Malicious App detection with Machine Learning-based Lightweight Cloud based scanning.		
Device Compliance	Easily check if a new mobile device is compliant with certain policy.	<ul style="list-style-type: none"> <li>Partner-Vendor</li> </ul>	Existing solution
Virtual Private Network (VPN)	Ensures privacy of communication by encrypting all mobile and IoT devices traffic.	<ul style="list-style-type: none"> <li>Acronis</li> <li>Partner-Vendor</li> <li>Partner-University/Research Center</li> </ul>	Research
Data Leakage Detection	Provides visibility of potential application data leakage via network traffic quota analysis.		
Network Security	Advanced security features for Service Providers covering highly-regulated verticals e.g. block untrusted Wi-Fi access points for IoT and mobile devices.		
Phishing Prevention	Automated detection of malicious websites and protecting the user from opening them.	<ul style="list-style-type: none"> <li>Acronis</li> </ul>	V
Built-in solution	Provide solution pre-installed on mobile devices, so they are protect from day one.	<ul style="list-style-type: none"> <li>Partner-Vendor</li> </ul>	Deployment

# European Mobile Cyber Protection - Consortia & Timeline



The **consortia** is open for the telecoms and mobile device management (MDM)-vendors as well as for academic institutions and research centers/groups in the field of:

- IoT and Mobile Device Management
- Device Compliance
- Virtual Private Network (VPN)
- Data Leakage Detection
- Network Security
- Built-in solution

**Performance timeline** from the date consortia is formed (July Y2023): 36 months



# Acronis - Contact details



**For more information and for interest to participate please contact:**

Name and affiliation: Plamen Toshev, Acronis Bulgaria  
E-Mail: [vlad.dv@acronis.com](mailto:vlad.dv@acronis.com)  
Telephone: + 359 877 200 693  
Postal Address: Bulgaria, Sofia, 59 G.M. Dimitrov blvd,  
NV Tower, Sofia, Bulgaria 1700



**Acronis**

**Web:** [www.acronis.com](http://www.acronis.com)

Presentation available via request on: [vlad.dv@acronis.com](mailto:vlad.dv@acronis.com)





# 14th Dec. 16 CET

## Join the follow-up Telco

[Join meeting](#)

Join by meeting number

Meeting number (access code): 2740 289 4899

Meeting password: F3iJN5b2Jq7

Join by phone

+49-6196-7819736 Germany Toll

[Can't join the meeting?](#)

