

A man with grey hair, wearing a blue button-down shirt, is smiling and talking on a mobile phone. He is positioned in front of a window with blinds, looking out to the right. The background is slightly blurred, showing the window frame and some outdoor elements.

**SECURING THE  
MOBILE-FIRST  
BUSINESS**

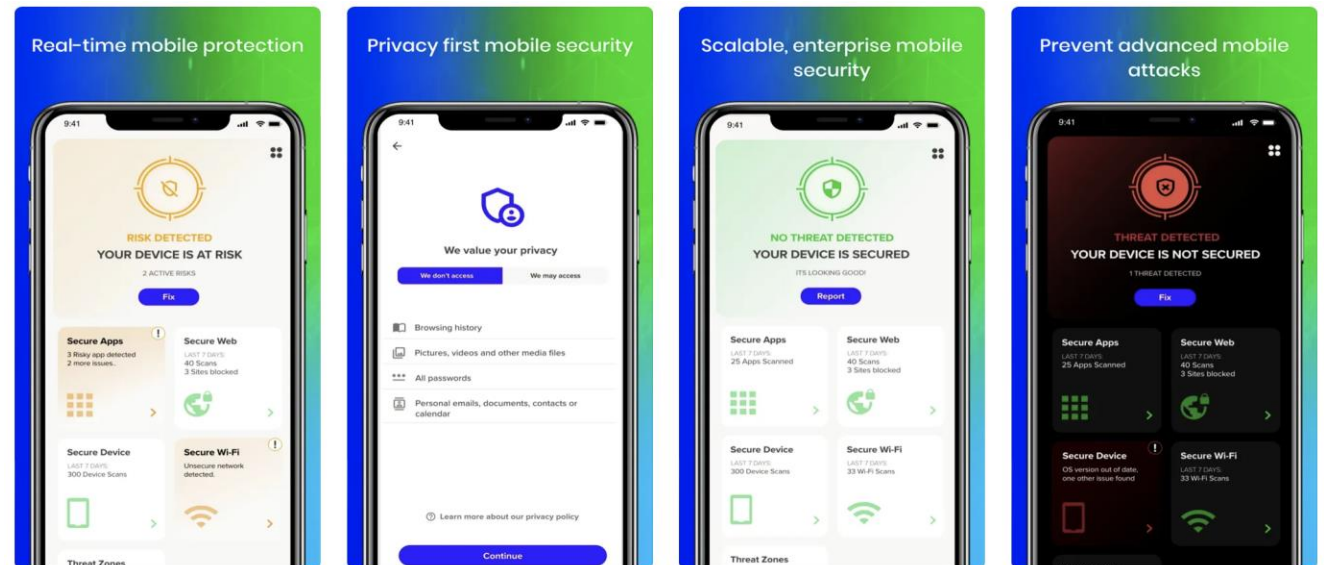


# What We Do

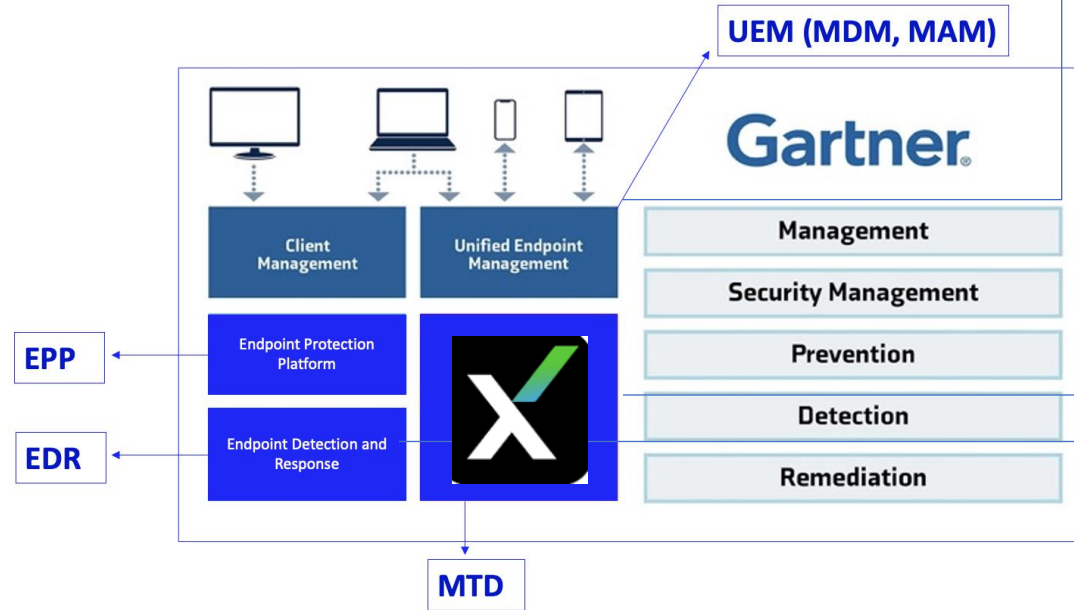


**Trellix Mobile Security**  
Business

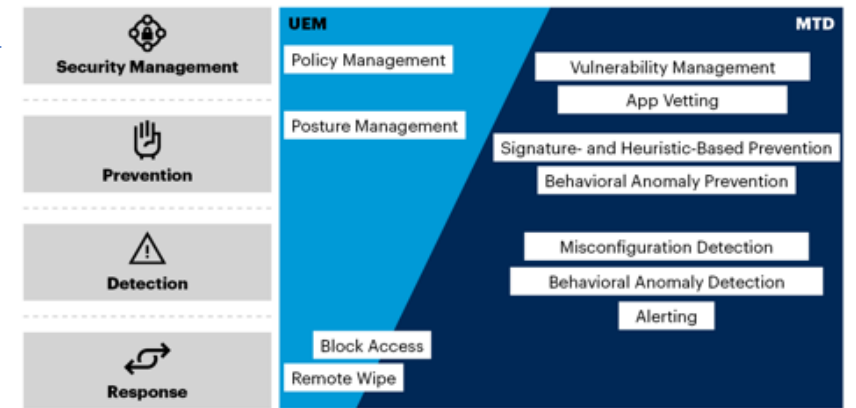
Zimperium **secures mobile devices and applications** so they can access enterprise data in a safe and secure manner.



# Why are we in Trellix Mobile



**Mobile Threat Defense Functionality Compared With That of Unified Endpoint Management**



Source: Gartner  
749863\_C

Gartner

**XDR Implementation With Support for iOS and Android via an MTD Solution**



Source: Gartner  
736793\_C

Gartner

An aerial, high-angle photograph of a crowd of people walking across a crosswalk. The crosswalk is marked with white stripes on a dark pavement. The people are seen from above, moving in various directions. The overall tone is dark and somewhat somber.

**“Why MFA on a mobile device... is NOT  
the silver bullet in a zero trust  
architecture... without VISIBILITY!”**

- Zimperium, 2023

# Who remembers these?



RSA SecurID SD600



RSA SecurID SID700



RSA SecurID SD200



RSA SecurID SD520

## Why did we trust them?



Device



Network



Applications



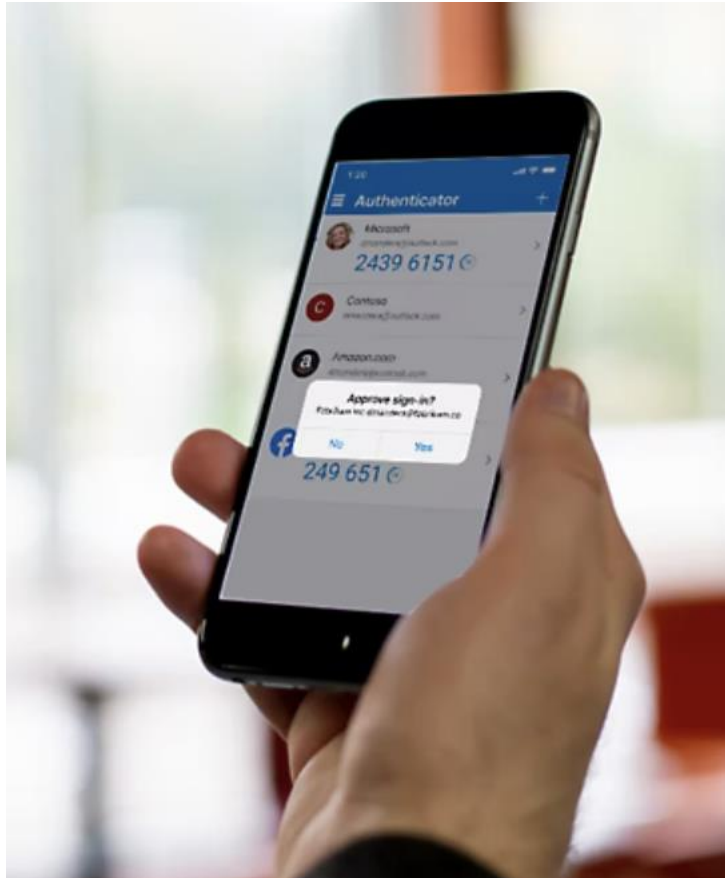
Phishing

# So why would you trust **these?**

Attacks by bad actors



Risks from employees



**Device**

**65%**

*Avg. % of enterprise devices running an OS with CRITICAL vulnerabilities*



**Network**

**1:5**

*One in five enterprise mobile devices experienced a network attack*



**Applications**

**144,000**

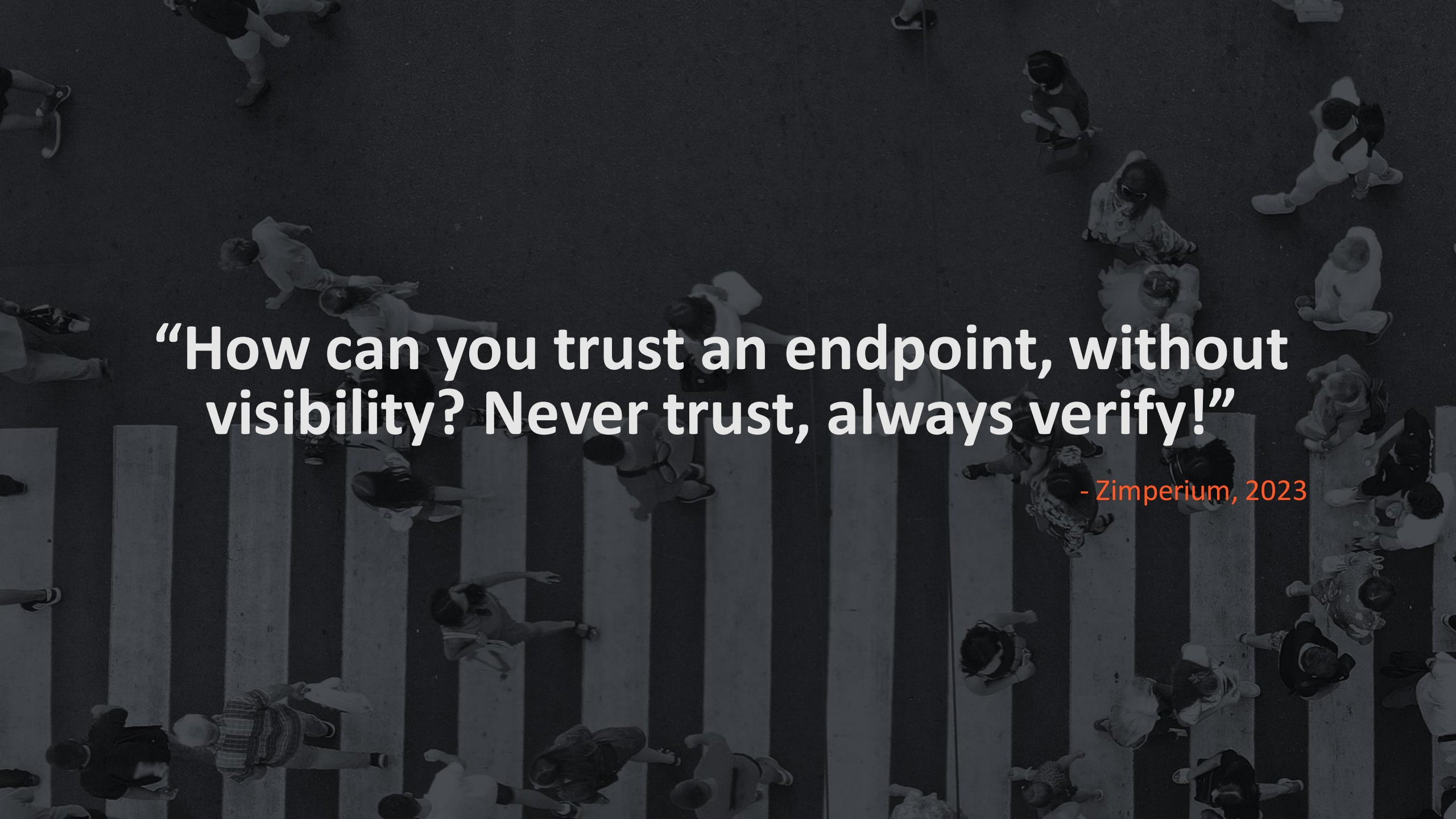
*New mobile malware per month<sup>1</sup>*



**Phishing**

**90/60**

*90% of breaches start with phishing;  
60% of emails read on mobile*

An aerial, high-angle photograph of a large crowd of people crossing a zebra crossing. The crossing is marked with white stripes on a dark asphalt surface. The people are seen from above, moving in various directions across the crossing. The overall tone is dark and somewhat somber.

**“How can you trust an endpoint, without visibility? Never trust, always verify!”**

- Zimperium, 2023

# Example: How do you handle **phishing / smishing** on mobile?



What technological controls on mobile do you have to prevent phishing or smishing?

**E-mail gateway!**

**? SMS, Slack, Teams, WhatsApp, Personal mail,...**

**No worries!**

**We trained our users!**



# Awareness training: Phishing / smishing messages have spelling mistakes in them!

Subject: URGENT: Account at Risk!

Hi [Recipient's Name],

Your account is in danger of suspension! 🚨

Click this link NOW to resolve: [Insert Link]

Act fast to keep your access!

Enter



Dear [Recipient's Name],

We hope this message finds you well. We need your immediate attention to a matter of utmost importance regarding your account. Failing to take action promptly could result in the suspension of your account, which we understand is something you'd like to avoid.

To prevent any disruption to your services and maintain uninterrupted access, please click on the following link right away: [Insert Link]

This link will guide you through the necessary steps to resolve the issue at hand. Time is of the essence, and we urge you to act swiftly to ensure your account remains active and fully functional.

If you have any questions or require assistance during this process, our dedicated support team is standing by to help. Please do not hesitate to reach out to us at [Support Email] or [Support Phone Number].

We appreciate your immediate attention to this matter and thank you for being a valued member of our community. Your prompt action will ensure a seamless experience with our services.

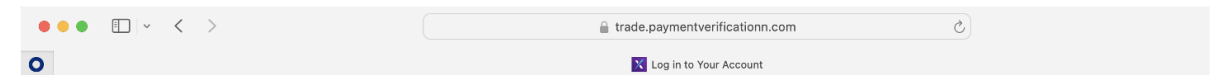
Sincerely,

[Your Name] [Your Title] [Company Name] [Contact Information]

# Awareness training:

We ask users to inspect the URL before clicking it!

Original : <https://www.trade.paymentverificationn.com>



bitly



Enter

Result : <https://bit.ly/45nln1Z>



# Why now? Recent use cases:

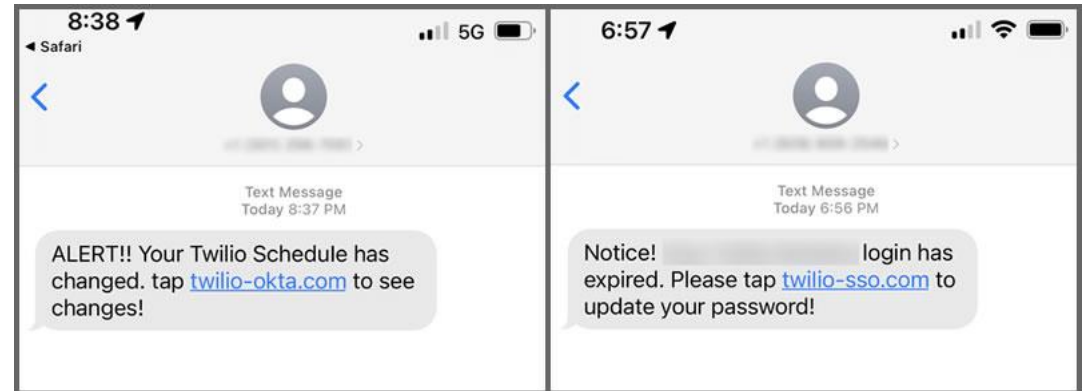
# Uber




(I was spamming employee with push auth for over a hour) i then contacted him on WhatsApp and claimed to be from Uber IT, told him if he wants it to stop he must accept it 6:47 PM

And well, he accepted and I added my device 6:47 PM

MFA Fatigue



Smishing

An aerial, top-down view of a crowd of people walking across a crosswalk. The crosswalk consists of several thick, parallel white stripes on a dark asphalt surface. The people are seen from above, some walking in different directions, some looking down at their phones. The overall scene is in grayscale, with the text overlaid in white and orange.

**“How Zimperium and Trellix Mobile can help you create visibility on” mobile apps and mobile devices!**

**Phishing  
Mobile Device Posture  
App vetting**

- Zimperium, 2023

An aerial, high-angle photograph of a diverse crowd of people crossing a zebra crossing. The scene is captured in a dark, monochromatic style with a semi-transparent black overlay. The white stripes of the zebra crossing are prominent, creating a grid-like pattern over the crowd. The people are seen from above, moving in various directions across the crossing. The overall mood is busy and public.

**“Your credentials are the keys to the  
kingdom!  
Here is why!”**

- Zimperium, 2023

# PHISHING: Do not expose your MFA to vulnerable devices! (example RSA)

Most hackers don't BREAK in, they LOG in

2003

RSA owns 70% of MFA market with 25 million devices



Dedicated hardware generating a 60 seconds personal access code

TODAY

Scattered landscape: Multiple vendors having a TAM of 12,9 billion USD



More than 80% of the market is software based (do you trust the device it runs on?!)

TODAY

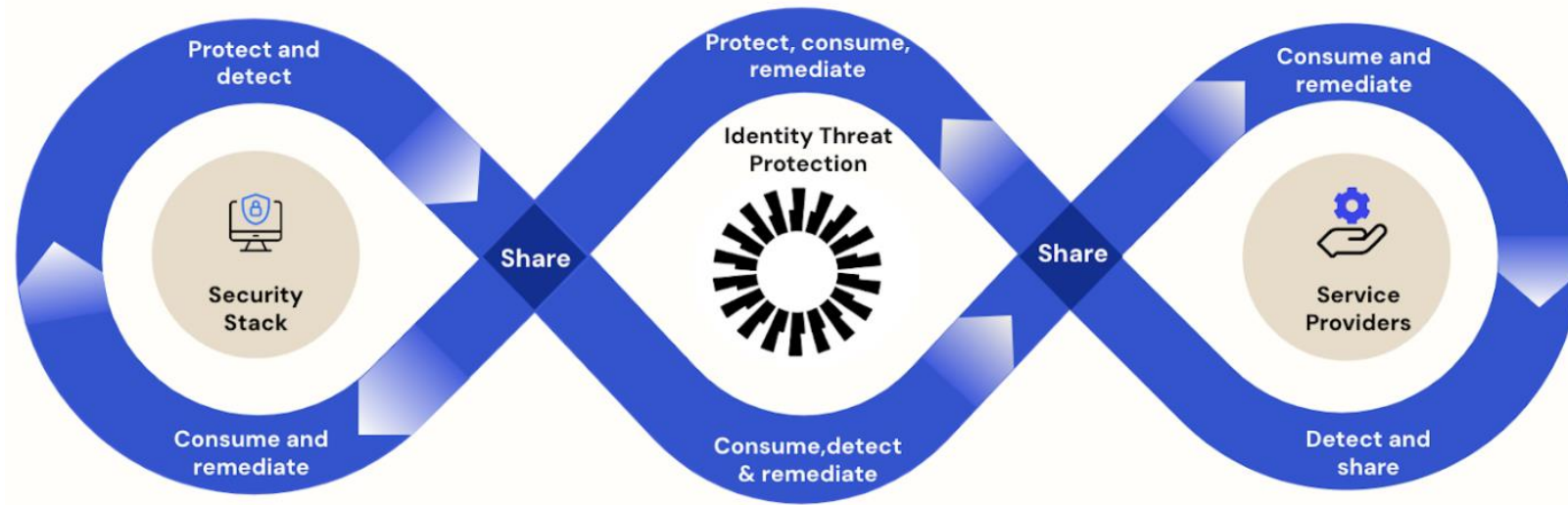
RSA announces Mobile Lock while partnering with Zimperium



The solution provides mobile device attestation, before allowing authentication

# MOBILE DEVICE POSTURE: Never Trust, Always Verify (Zero Trust) (example Okta)

Okta Identity Protection with Okta AI




Best-of-breed technology partners




# APP VETTING: Your OWN and THIRD PARTY mobile apps

**Trellix** Technical Summary


---



**TikTok 29.8.4**  
 com.zhillaapp.musically  
 b2c810d6e810495501e4e82f7d4f13fb  
 Scan Engine Version: 2.6.7  
 Scan Date: 06-08-2023



**LOW**  
Privacy Risk




**MED**  
Security Risk

This Technical Summary contains a mid-level summary and score information for an app's identified risk conditions. This digest is intended for a technical audience and provides a listing of items we identified. Findings are separated into analysis areas, followed by categories and additional support details when available. Each finding is represented by a Red, Orange, Yellow or Green colored square.

- Red indicates a high level of risk and used to indicate when a test has failed.
- Orange indicates a moderate level of risk
- Yellow indicates a low risk or informational finding
- Green indicates that no risk conditions were identified and used to indicate when a test has passed.

| Name  | Location    | Last Sighted | Last Sighted Version | Last Build | Created ↓  |
|---|-------------|--------------|----------------------|------------|------------|
| <input type="checkbox"/> Unprotected Content Provider | classes.dex | 4 days ago   | 1.4                  | 4          | 4 days ago |








**Name** Unprotected Content Provider 

**Location** classes.dex

**Category** Vulnerability


**Subcategory** Components

**Severity** HIGH

| Severity ↓  | Finding Name                   | Description                   | Count | Accepted | Issue Status | Version | Platform  |
|---|--------------------------------|-------------------------------|-------|----------|--------------|---------|---|
| <input type="checkbox"/> <span style="background-color: #28a745; color: white; padding: 2px;">BEST PRACTICES</span> | Keyboard Cache Disabled        |                               |       |          |              |         |   |
| <input type="checkbox"/> <span style="background-color: #28a745; color: white; padding: 2px;">BEST PRACTICES</span> | Uses Certificate Pinning       | This app has implemente...    | 5     | No       | Open         | 1.4     |    |
| <input type="checkbox"/> <span style="background-color: #28a745; color: white; padding: 2px;">BEST PRACTICES</span> | IPC Configuration              |                               | 1     | No       | Open         | 1.4     |    |
| <input type="checkbox"/> <span style="background-color: #28a745; color: white; padding: 2px;">BEST PRACTICES</span> | Sensitive Data Protection      |                               | 5     | No       | Open         | 1.4     |    |
| <input type="checkbox"/> <span style="background-color: #28a745; color: white; padding: 2px;">BEST PRACTICES</span> | Chain of Trust Validation      |                               | 1     | No       | Open         | 1.4     |  |
| <input type="checkbox"/> <span style="background-color: #28a745; color: white; padding: 2px;">BEST PRACTICES</span> | Jailbreak and Root Detection   | This application has code...  | 1     | No       | Open         | 1.4     |  |
| <input type="checkbox"/> <span style="background-color: #ff9900; padding: 2px;">HIGH</span>                         | Debuggable App                 | This application has the "... | 1     | No       | Open         | 1.4     |  |
| <input type="checkbox"/> <span style="background-color: #ff9900; padding: 2px;">HIGH</span>                         | Non-escaped SQL functions used |                               | 3     | No       | Open         | 1.4     |  |

**Bundle Id** infosecadventures.allsafe

**Name** Allsafe

**Platform** 

**Created** 7 Oct 2023 19:18

**Finding Name** Unprotected Content Provider

**Severity** HIGH

**Category** Vulnerability

**Subcategory** Components


**Accepted** False


**Issue Status** Open


**Finding** The content provider is not protected by signature permission and is exported in the AndroidManifest.xml file. Content providers offer a structured storage mechanism that can be limited to this app or exported to allow access by other apps.

**Business Impact** An attacker can read or write the exported content provider, resulting in leakage of sensitive information or unpredictable app behavior. If the content providers are used as interfaces for a database, the attacker can access and potentially extract, update, insert, and delete information. In addition, there might be options for SQL injection and path traversal attacks.

**Recommendation** If other apps should not have access to this content provider, mark them as "android:exported=false" in the application manifest. Otherwise, set the "android:exported" attribute to true to allow other apps to access the stored data.

**App Name** Allsafe 

**Platform** 

**Instances** 1 

**Created** 4 days ago

**Modified** 4 days ago



An aerial, top-down view of a large crowd of people crossing a zebra crossing. The crossing is marked with white stripes on a dark asphalt surface. The people are seen from above, moving in various directions across the crossing. The overall scene is dimly lit, with a dark, monochromatic color palette.

**“Mobile ransomware is now a legitimate threat.”**

- Zimperium, 2023

# BEST PRACTICES: How to vet your Mobile Apps?

## THIRD PARTY APPS

The screenshot shows a 'Policy Builder' interface. On the left, under 'Available Characteristics', there is a search bar containing 'chatGPT'. Below it, a dropdown menu is open, showing 'Privacy' with the description 'The app is using OpenAI's ChatGPT'. On the right, under 'Policy Characteristics', there is a search bar containing 'Cloud Services' with the description 'Access a vulnerable AWS cloud instance'. Below it, another dropdown menu is open, showing 'Any Characteristics'. At the bottom right, it says 'Matches 28 Of 31768 Apps'.

**1. Review app characteristics**

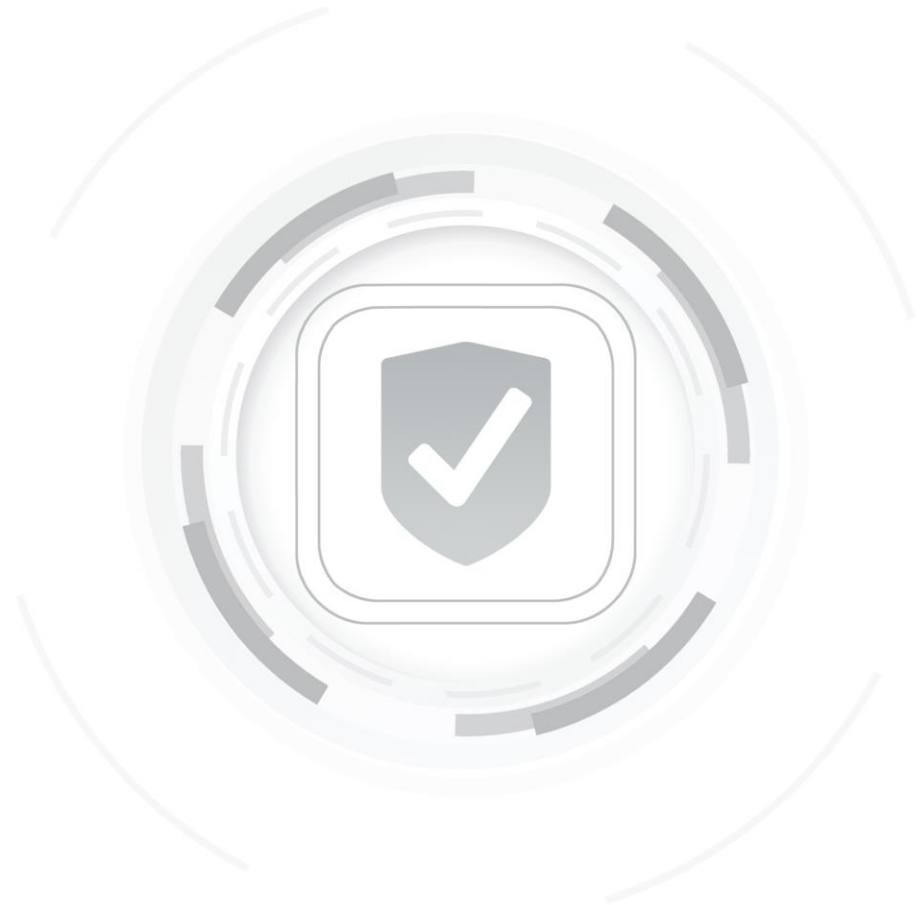
**2. Review privacy and security risks per app**


The screenshot shows the 'Trellix' logo and 'Technical Summary' header. Below the header, there is a section for 'TikTok 29.8.4' with the following details: 'com.zhiliaoapp.musically', 'b2c810d6e810495501e4e82f7d4f13fb', 'Scan Engine Version: 2.6.7', and 'Scan Date: 06-08-2023'. To the right of this section, there are two risk indicators: 'LOW Privacy Risk' (represented by a green padlock icon) and 'MED Security Risk' (represented by an orange shield icon). Below these indicators, there is a paragraph of text explaining the technical summary and a bulleted list of risk levels: 'Red indicates a high level of risk and used to indicate when a test has failed.', 'Orange indicates a moderate level of risk', 'Yellow indicates a low risk or informational finding', and 'Green indicates that no risk conditions were identified and used to indicate when a test has passed.'

# **BEST PRACTICES: How to vet your Mobile Apps?**

## *YOUR OWN APPS*

- 1. Build securely*
- 2. Protect your secrets*
- 3. Release securely*
- 4. Know your environment*



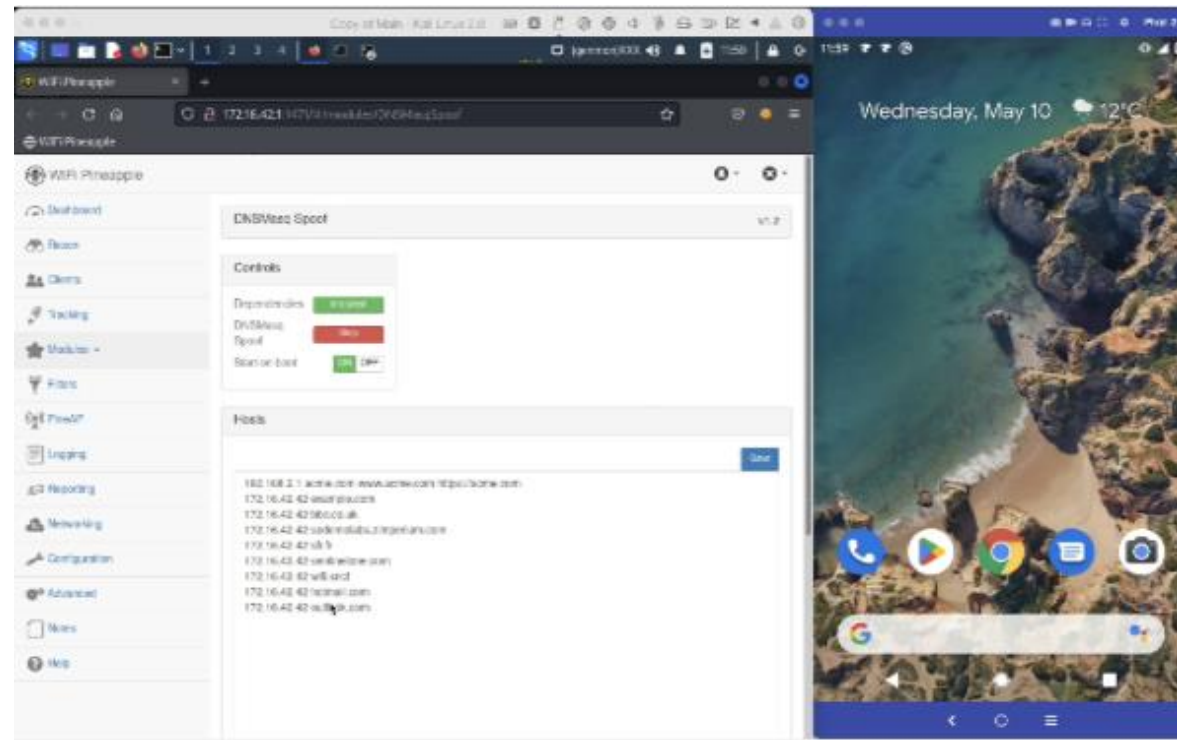
An aerial, high-angle photograph of a diverse crowd of people walking across a crosswalk. The crosswalk is marked with white vertical stripes on a dark asphalt surface. The people are seen from above, moving in various directions. The overall image has a dark, monochromatic aesthetic with a slight blue-grey tint.

**“When people, process and technology fail, attackers take advantage of it!  
Here is how!”**

- Zimperium, 2023

# Example: What does **Pegasus-like infection** a look like?

Live Demo:  
Key logging  
**SMS / MFA exfiltration**  
App behaviour



# Why now? Example: How will the **NIS2 directive** apply to mobile endpoints?

## **Article 6.b. - Definitions:**

What is a network and information system?



“any device or group of interconnected or related devices, one or more of which, pursuant to a program, carry out automatic processing of digital data”

## **Article 21 - Cybersecurity risk-management measures:**

What needs to be done?

- ✓ Policies on risk analysis and information system security
- ✓ Incident handling
- ✓ Supply chain security
- ✓ Policies and procedures to assess the effectiveness of cybersecurity risk management measures
- ✓ Policies and procedures regarding the use of cryptography and encryption

## **Article 23 – Reporting obligations:**

What and when (72 hours) needs to be reported?

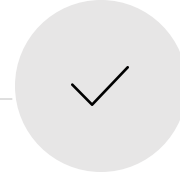
(j) the use of multi-factor authentication or continuous authentication solutions emergency communication systems within the entity, where appropriate.

- ✓ Potential unlawful or malicious acts or cross-border impact
- ✓ An initial assessment, including severity, impact, and known indicators of compromise

# Recommended Next Steps

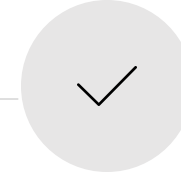


Understand why  
mobile device and  
app posture is key



Vet your Mobile App

Receive a personalized app analysis  
of YOUR mobile app



Test For Yourself

Pilot the solution internally to  
validate enterprise fit

# 2023 Global Mobile Threat Report Now Available







Advanced **Mobile**  
**Security** for  
Enterprises

