SIA Session 3: Zimperium Studio 4

Your data is mobile. Is your security?

Marcos REGIDOR
Director Technical Sales

Geert NOBELS
Tribe Leader EMEA
CISSP CCSP CISM CISA CDPSE CCAK CCSK

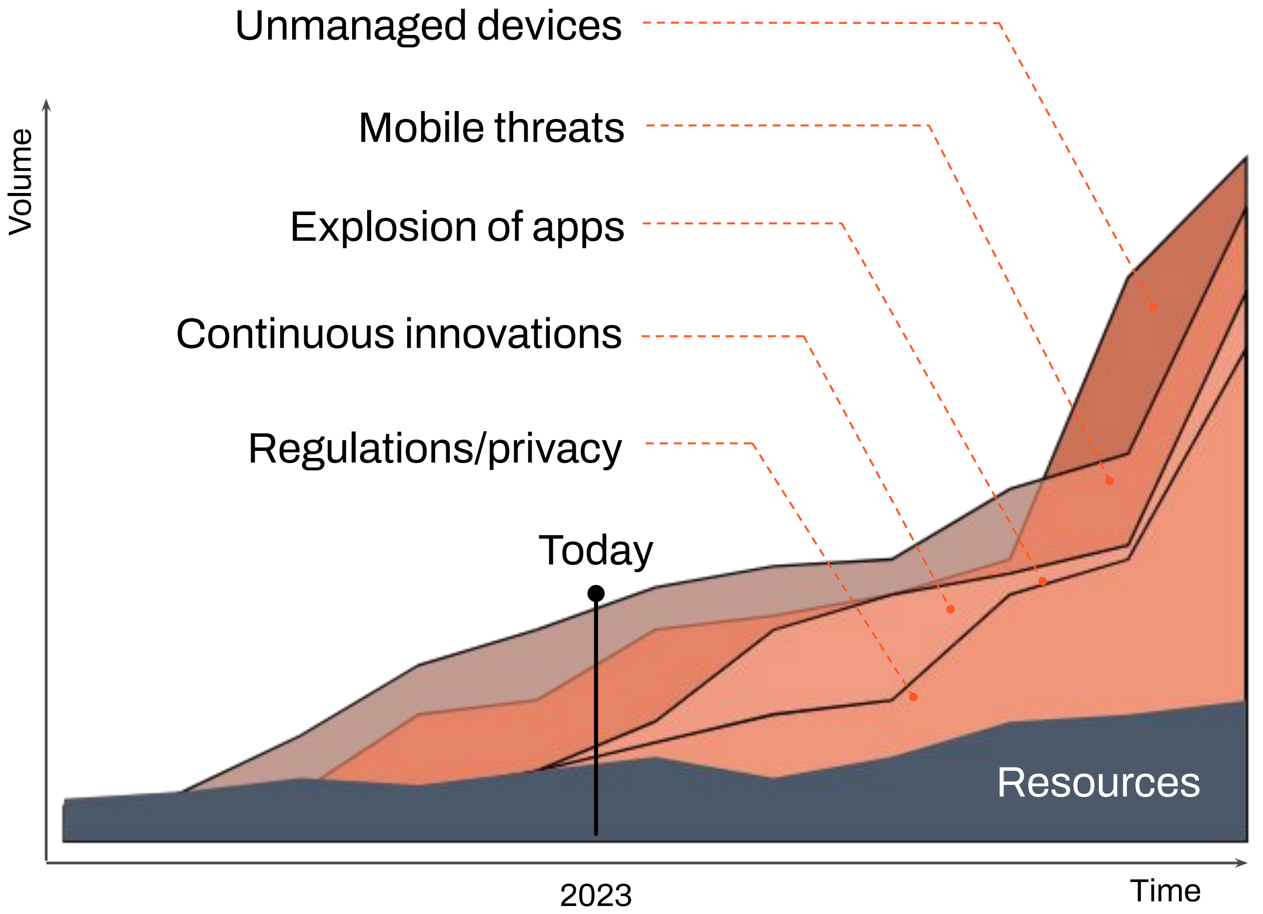
Mobile Cyber Hygiene

“How can you trust mobile, without visibility?”

Never trust, always verify!

RISK MOVES TO THE EDGE

The escalating Vulnerability Gap



Vulnerability Gap

| uncontrolled
| blind spots
| exposure points

Creating negative consequences

BRAND IMPACT

46%

suffered reputational damage

FINANCIAL IMPACT

$29B

digital fraud from mobile

BOARD-LEVEL PRIORITY

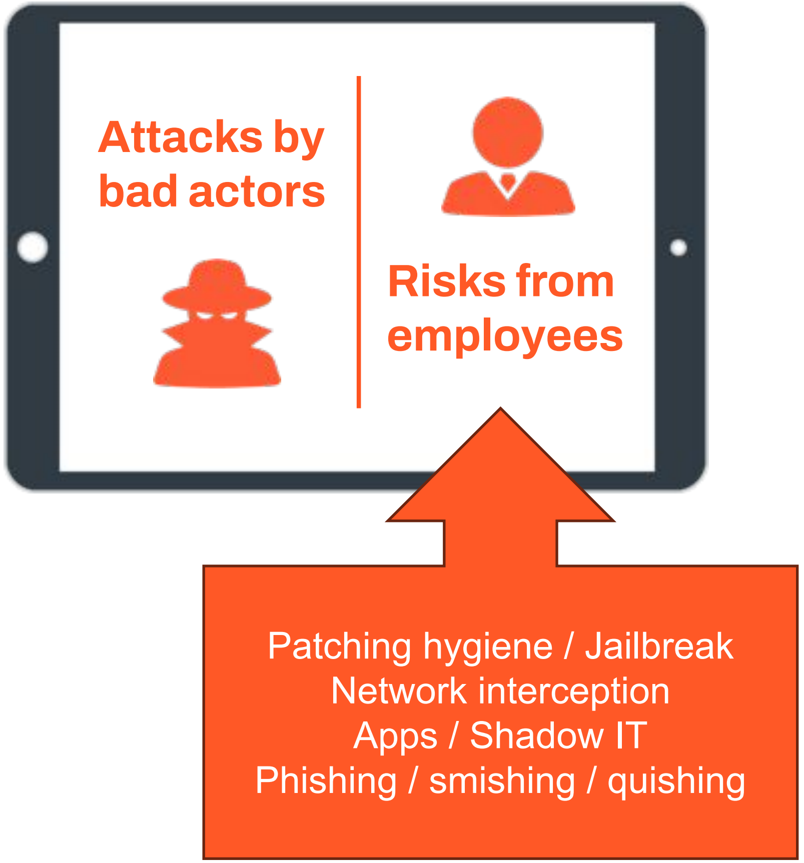
88%

view cyber risk as business risk

ZIMPERIUM.

Threat exposure for mobile devices

CYBER HYGIENE



Attacks by bad actors

Risks from employees

Patching hygiene / Jailbreak
Network interception
Apps / Shadow IT
Phishing / smishing / quishing

Device

65% *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 signatures per month

Phishing

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

OS exposure for mobile devices

COST OF DATA AND ACCESS TO POWER DICTATE PATCHING HYGIENE

Exploitation of OS or Kernel Vulnerabilities, Malicious Chargers, etc.

Manipulation of Encryption Keys, Integrity Checks, Libraries, System Calls, etc.

Remote Access

Rooting

Downloads & Executables

Mount Point Changes

Keychain Exposure

System Tampering

Privilege Escalation

Keylogger

File Decryption

Device

65% *of enterprise devices running an OS with CRITICAL vulnerabilities*

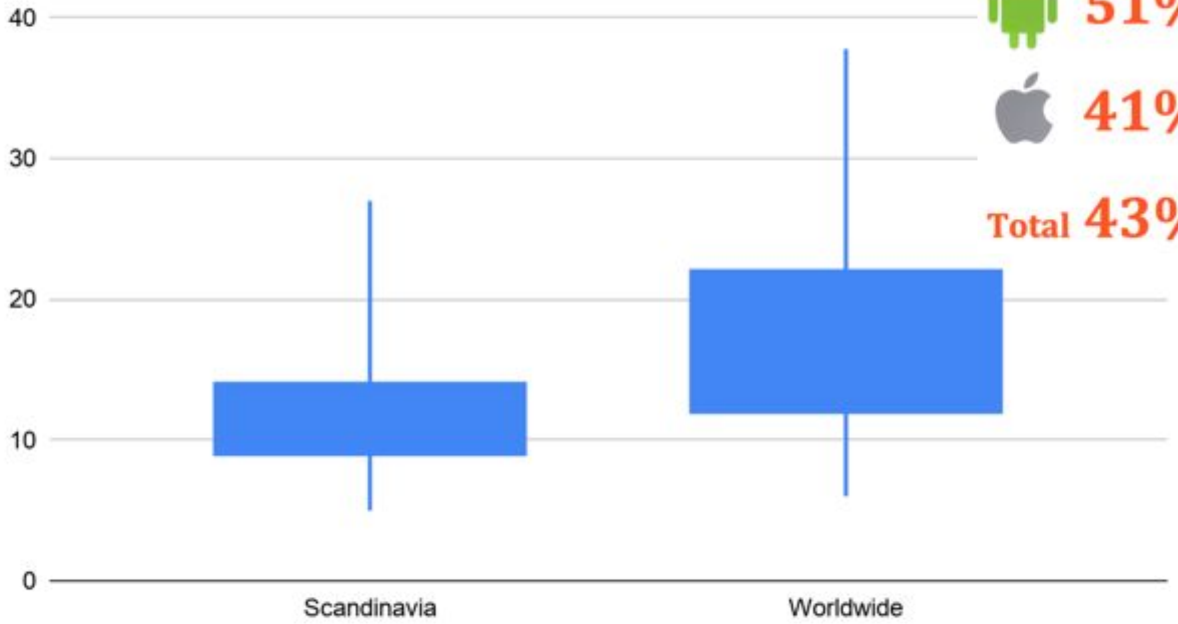
% tampered
not rooted/jailbroken

51%

41%

Total 43%

Time to update device from release (in days)



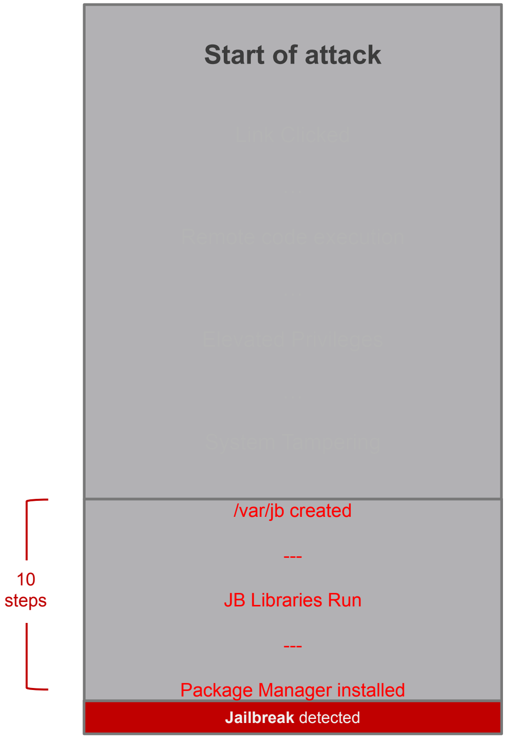
Defensive strategies: Compromise vs Root Detection

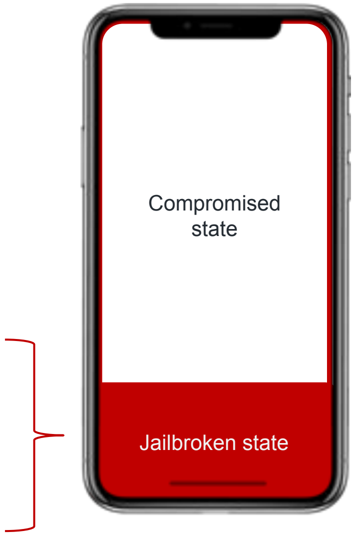
Zimperium focuses on detecting abnormalities, indicators of compromise, and advanced attack techniques. Other tools only trigger a detection when the final, already-known static steps of an attack are detected.

Other Jailbreak/Root Detection Tools

Does the “/var/jb” file path exist ✅
Are there known JB/Root libraries running ✅
Is there a known package manager installed ✅

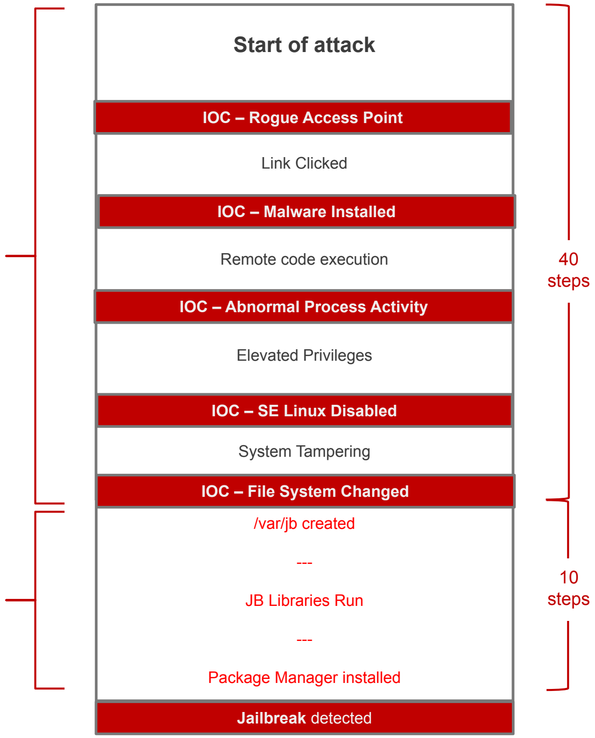
Jailbreak or Root detected, since the last known steps of an attack are completed.

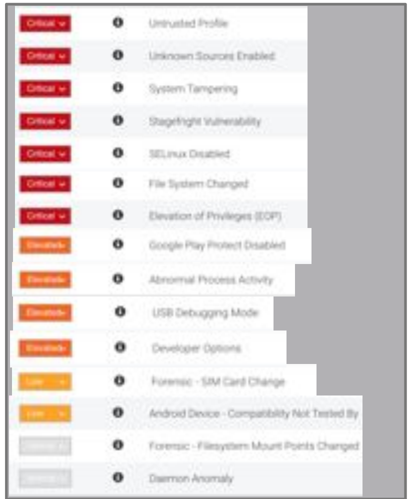




Example: Basic, known jailbreak or root tools.

Zimperium Compromise Detection





Critical	●	Untrusted Profile
Critical	●	Unknown Sources Enabled
Critical	●	System Tampering
Critical	●	Stagefright Vulnerability
Critical	●	SELinux Disabled
Critical	●	File System Changed
Critical	●	Elevation of Privileges (EOP)
Elevated	●	Google Play Protect Disabled
Elevated	●	Abnormal Process Activity
Elevated	●	USB Debugging Mode
Elevated	●	Developer Options
Low	●	Forensic - SIM Card Change
Low	●	Android Device - Compatibility Not Tested By
[illegible]	●	Forensic - Filesystem Mount Points Changed
[illegible]	●	Daemon Anomaly

✅ Evaluate System Security & state
✅ Check system privileges
✅ Check for modified files and Paths
✅ Check for malicious libraries or processes
✅ Check for package managers

❌ Does the “/var/jb” file path exist
❌ Are there known JB/Root libraries running
❌ Is there a known package manager installed

Jailbreak/Root is detected, in addition to a trail of compromise indicators which show an attack.

Defensive strategies: Compromise vs Root Detection

Zimperium focuses on detecting abnormalities, indicators of compromise, and advanced attack techniques. Other tools only trigger a detection when the final, already-known static steps of an attack are detected.

Other Jailbreak/Root Detection Tools

Does the "/var/jb" file path exist ❌

Are there known JB/Root libraries running ❌

Is there a known package manager installed ❌

Jailbreak or Root not detected, despite the device being compromised.

10 steps

Start of attack

Link Clicked

Remote code execution

Elevated Privileges

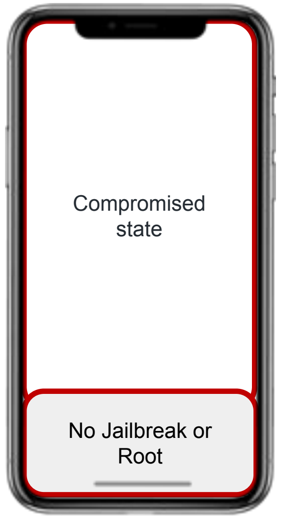
System Tampering

/var/jb created

JB Libraries Run

Package Manager installed

Jailbreak not detected



Example: Legitimate malicious, or Zero-day attacks.

It **compromises the device** but **does not jailbreak or Root device.**

Zimperium Compromise Detection

Start of attack

IOC – Rogue Access Point

Link Clicked

IOC – Malware Installed

Remote code execution

IOC – Abnormal Process Activity

Elevated Privileges

IOC – SE Linux Disabled

System Tampering

IOC – File System Changed

40 steps

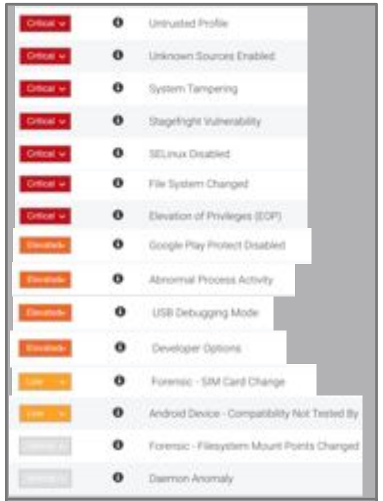
/var/jb created

JB Libraries Run

Package Manager installed

Jailbreak not detected

10 steps



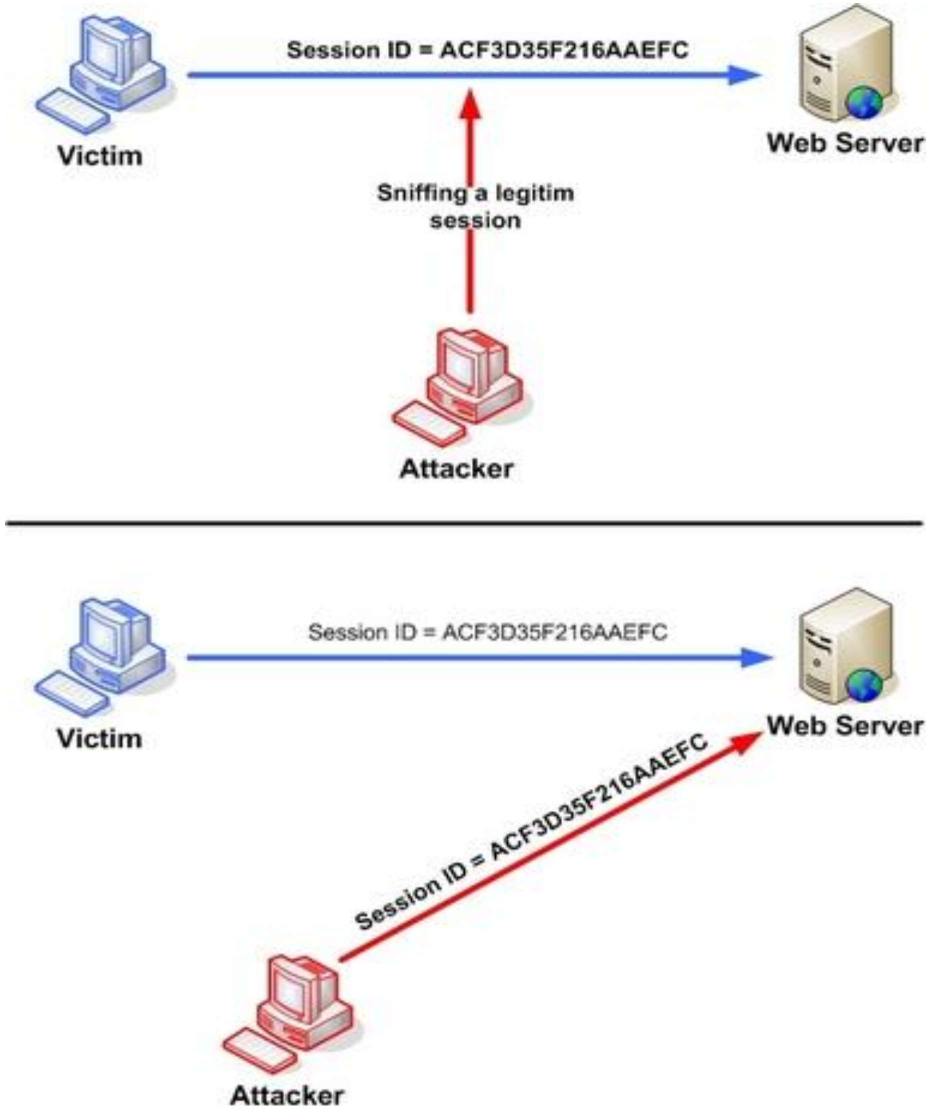
Critical	Untrusted Profile
Critical	Unknown Sources Enabled
Critical	System Tampering
Critical	Stagefright Vulnerability
Critical	SELinux Disabled
Critical	File System Changed
Critical	Elevation of Privileges (EOP)
Elevated	Google Play Protect Disabled
Elevated	Abnormal Process Activity
Elevated	USB Debugging Mode
Elevated	Developer Options
Low	Forensic - SIM Card Change
Low	Android Device - Compatibility Not Tested By
[illegible]	Forensic - Filesystem Mount Points Changed
[illegible]	Daemon Anomaly

✅ Evaluate System Security & state
✅ Check system privileges
✅ Check for modified files and Paths
✅ Check for malicious libraries or processes
✅ Check for package managers

❌ Does the "/var/jb" file path exist
❌ Are there known JB/Root libraries running
❌ Is there a known package manager installed

Jailbreak or Root is NOT detected. However, the trail of compromise indicators show an attack.

Network exposure for mobile devices


Session ID = ACF3D35F216AAEFC
Victim
Web Server
Sniffing a legitim session
Attacker
Session ID = ACF3D35F216AAEFC
Victim
Web Server
Session ID = ACF3D35F216AAEFC
Attacker

Device

65% *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 signatures per month

Phishing

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

https://owasp.org/www-community/attacks/Session_hijacking_attack

App exposure for mobile devices

THE NEW SHADOW IT COMPONENTS ARE MOBILE AND AI

Malware   3rd Party Libraries / Back Door

Dynamic Runtime Injection   Ransomware

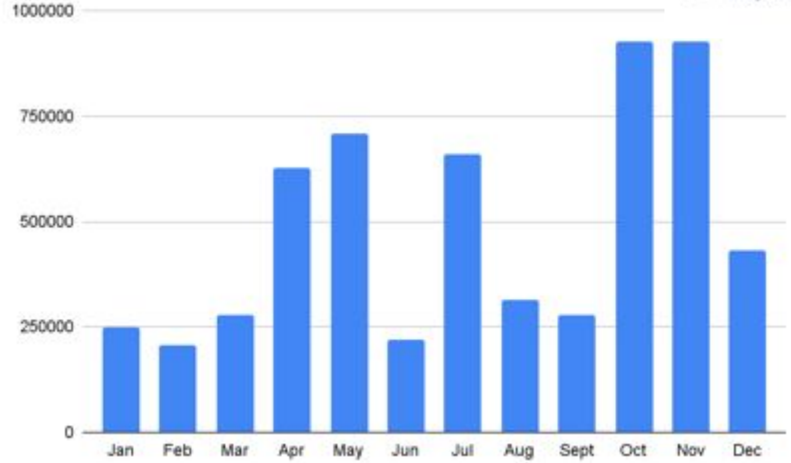
Remote Access Tools   Data Harvesting

Spyware   Browser CVEs   Trojans

Repackaged Apps   BankBots

EMEA

- Malware 57%
- Riskware 10%
- Trojan 8%



Device

65% *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

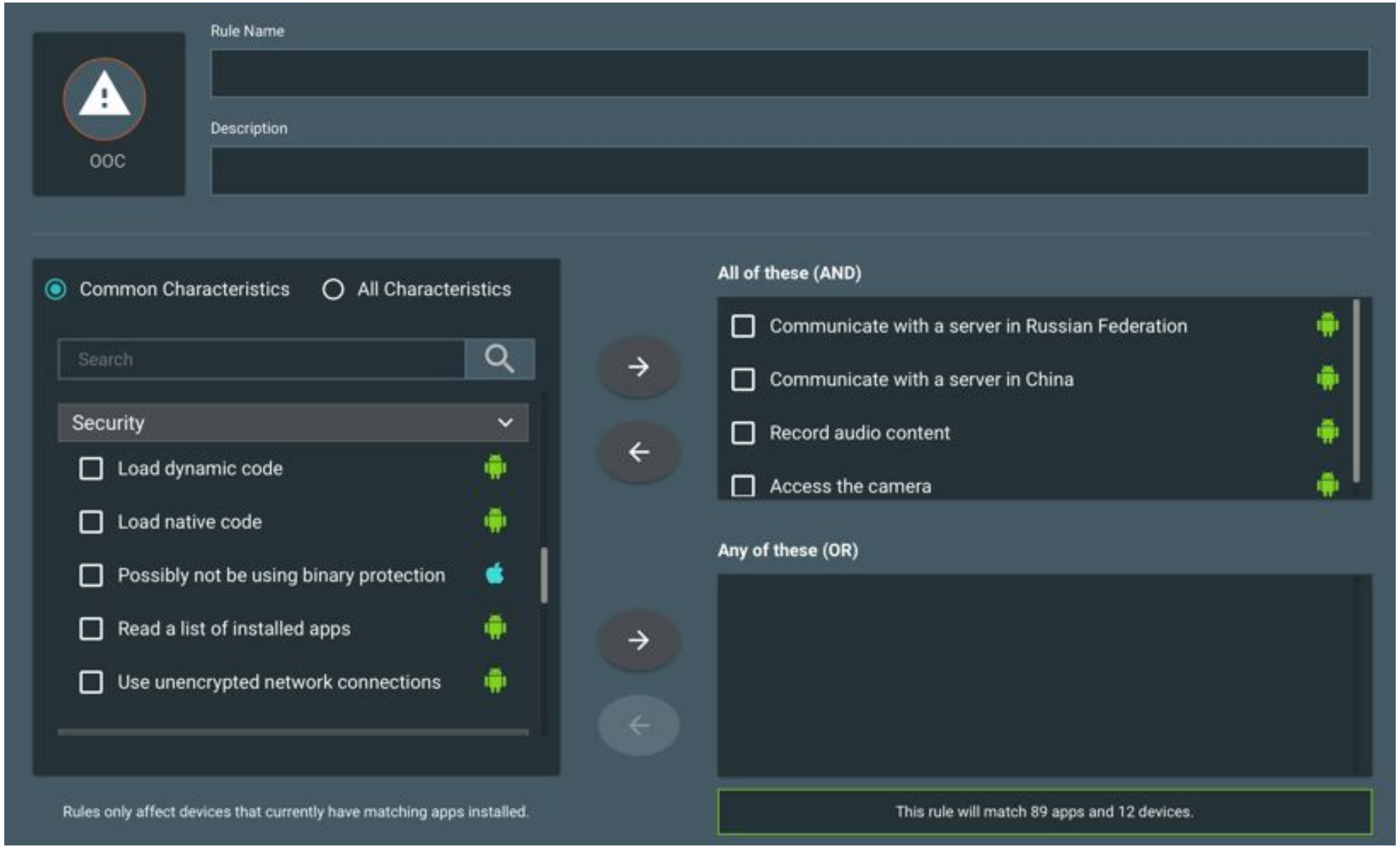
New mobile malware signatures per month

Phishing

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

App hunting and app vetting

LOOK FOR APP CHARACTERISTICS AND AFFECTED DEVICES



OOC

Rule Name

Description

● Common Characteristics ○ All Characteristics

Search

Security

- □ Load dynamic code
- □ Load native code
- □ Possibly not be using binary protection
- □ Read a list of installed apps
- □ Use unencrypted network connections

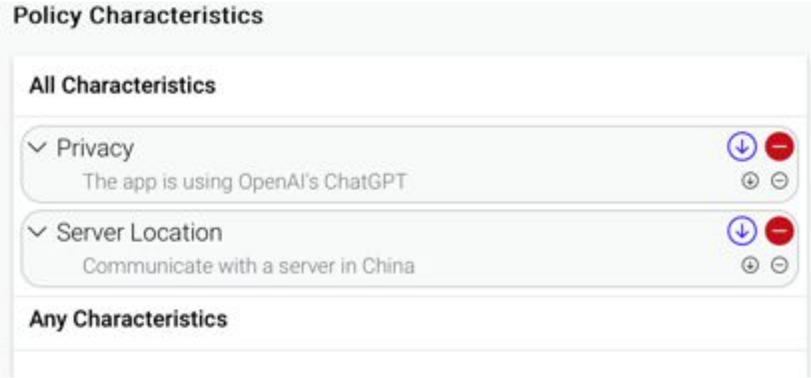
All of these (AND)

- □ Communicate with a server in Russian Federation
- □ Communicate with a server in China
- □ Record audio content
- □ Access the camera

Any of these (OR)

Rules only affect devices that currently have matching apps installed.

This rule will match 89 apps and 12 devices.



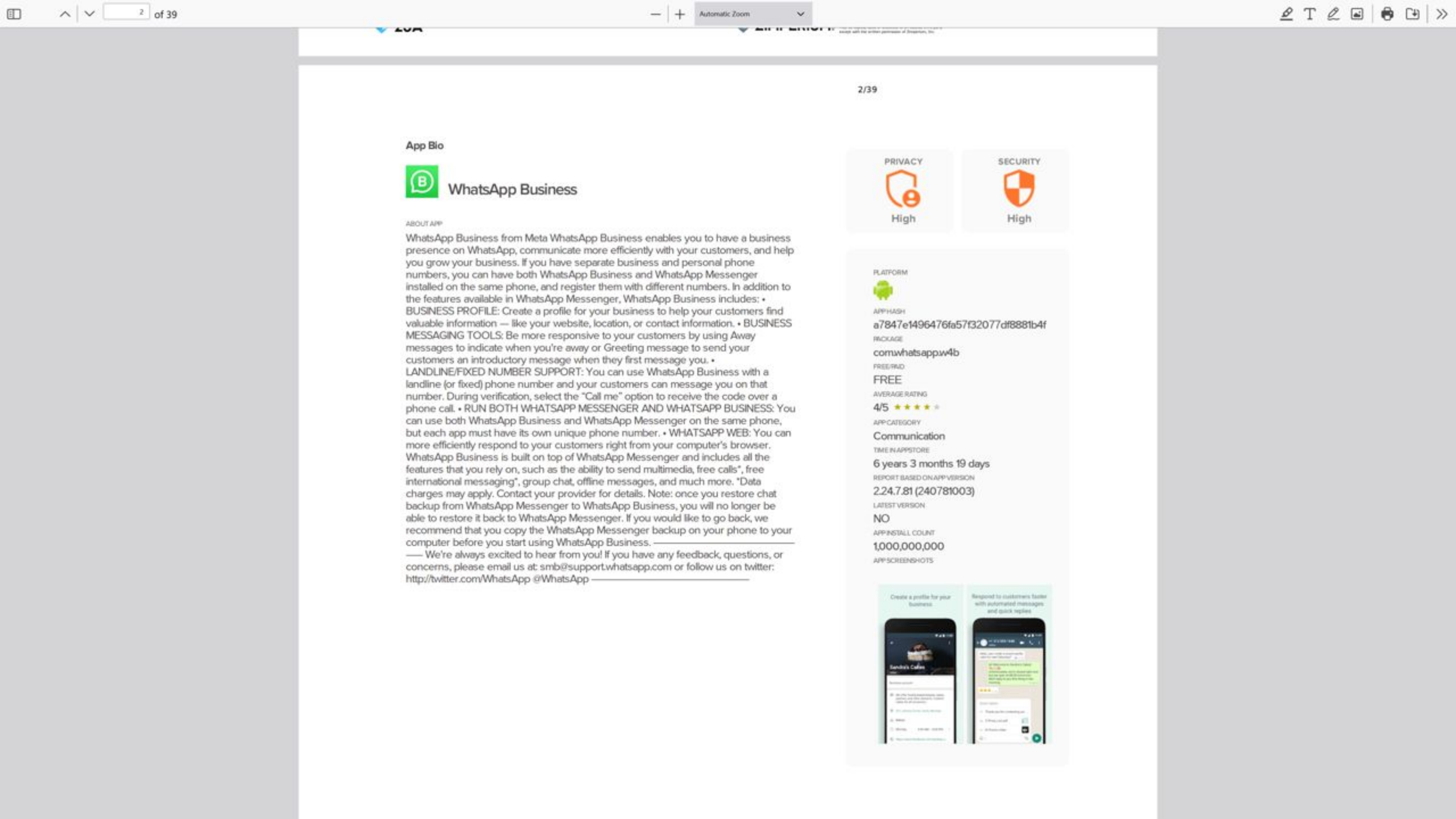
Policy Characteristics

All Characteristics

Privacy
The app is using OpenAI's ChatGPT

Server Location
Communicate with a server in China

Any Characteristics



App Bio

WhatsApp Business

ABOUT APP

WhatsApp Business from Meta WhatsApp Business enables you to have a business presence on WhatsApp, communicate more efficiently with your customers, and help you grow your business. If you have separate business and personal phone numbers, you can have both WhatsApp Business and WhatsApp Messenger installed on the same phone, and register them with different numbers. In addition to the features available in WhatsApp Messenger, WhatsApp Business includes: • BUSINESS PROFILE: Create a profile for your business to help your customers find valuable information — like your website, location, or contact information. • BUSINESS MESSAGING TOOLS: Be more responsive to your customers by using Away messages to indicate when you're away or Greeting message to send your customers an introductory message when they first message you. • LANDLINE/FIXED NUMBER SUPPORT: You can use WhatsApp Business with a landline (or fixed) phone number and your customers can message you on that number. During verification, select the "Call me" option to receive the code over a phone call. • RUN BOTH WHATSAPP MESSENGER AND WHATSAPP BUSINESS: You can use both WhatsApp Business and WhatsApp Messenger on the same phone, but each app must have its own unique phone number. • WHATSAPP WEB: You can more efficiently respond to your customers right from your computer's browser. WhatsApp Business is built on top of WhatsApp Messenger and includes all the features that you rely on, such as the ability to send multimedia, free calls*, free international messaging*, group chat, offline messages, and much more. *Data charges may apply. Contact your provider for details. Note: once you restore chat backup from WhatsApp Messenger to WhatsApp Business, you will no longer be able to restore it back to WhatsApp Messenger. If you would like to go back, we recommend that you copy the WhatsApp Messenger backup on your phone to your computer before you start using WhatsApp Business. ——————————————————— We're always excited to hear from you! If you have any feedback, questions, or concerns, please email us at: smb@support.whatsapp.com or follow us on twitter: http://twitter.com/WhatsApp @WhatsApp ————————————————————

PRIVACY

High

SECURITY

High

PLATFORM

APP HASH

a7847e1496476fa57f32077df8881b4f

PACKAGE

com.whatsapp.w4b

FREE/PAID

FREE

AVERAGE RATING

4/5 ★★★★☆

APP CATEGORY

Communication

TIME IN APPSTORE

6 years 3 months 19 days

REPORT BASED ON APP VERSION

2.24.7.81 (240781003)

LATEST VERSION

NO

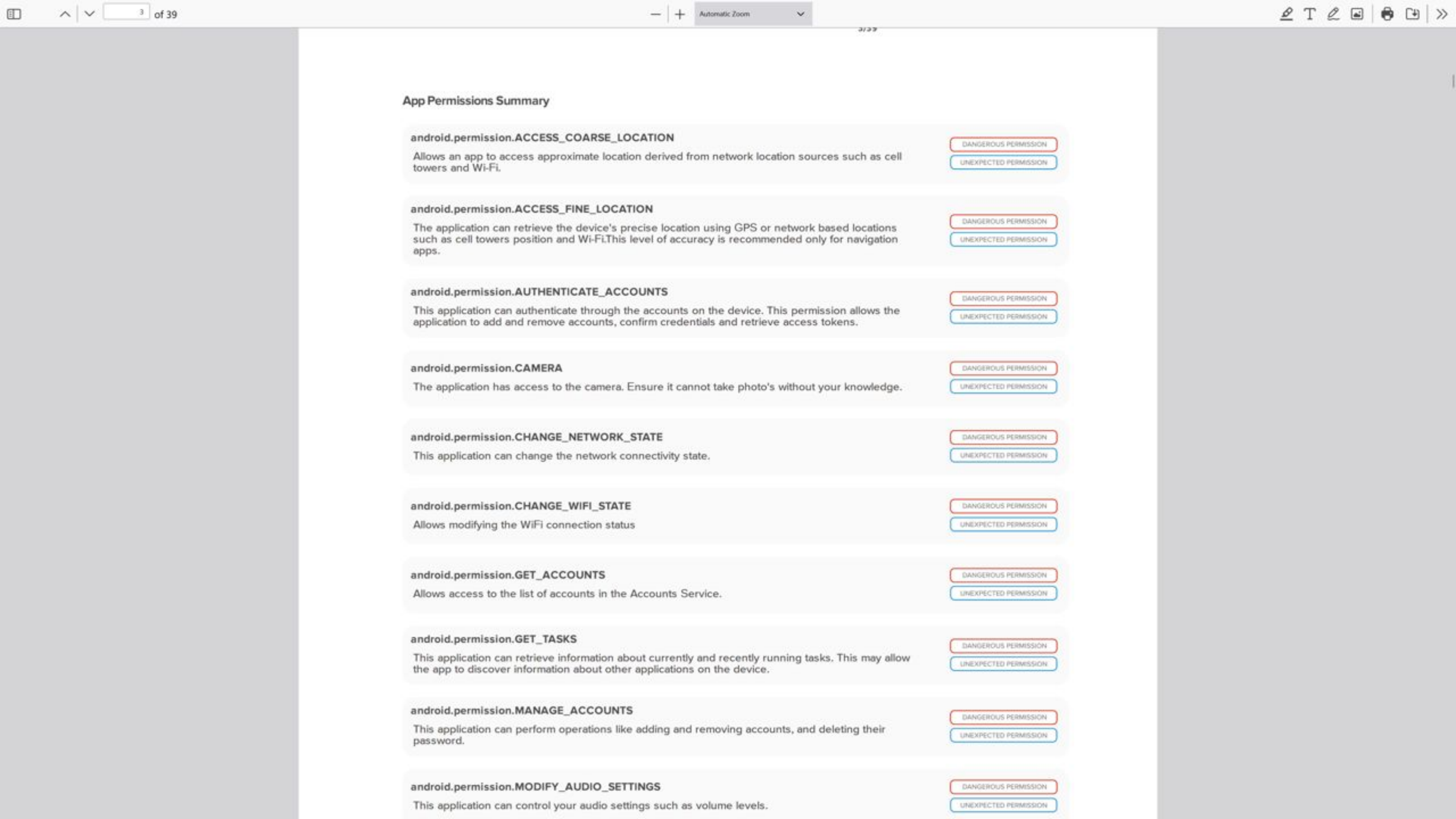
APP INSTALL COUNT

1,000,000,000

APP SCREENSHOTS

Create a profile for your business

Respond to customers faster with automated messages and quick replies



App Permissions Summary

android.permission.ACCESS_COARSE_LOCATION

Allows an app to access approximate location derived from network location sources such as cell towers and Wi-Fi.

DANGEROUS PERMISSION
UNEXPECTED PERMISSION

android.permission.ACCESS_FINE_LOCATION

The application can retrieve the device's precise location using GPS or network based locations such as cell towers position and Wi-Fi.This level of accuracy is recommended only for navigation apps.

DANGEROUS PERMISSION
UNEXPECTED PERMISSION

android.permission.AUTHENTICATE_ACCOUNTS

This application can authenticate through the accounts on the device. This permission allows the application to add and remove accounts, confirm credentials and retrieve access tokens.

DANGEROUS PERMISSION
UNEXPECTED PERMISSION

android.permission.CAMERA

The application has access to the camera. Ensure it cannot take photo's without your knowledge.

DANGEROUS PERMISSION
UNEXPECTED PERMISSION

android.permission.CHANGE_NETWORK_STATE

This application can change the network connectivity state.

DANGEROUS PERMISSION
UNEXPECTED PERMISSION

android.permission.CHANGE_WIFI_STATE

Allows modifying the WiFi connection status

DANGEROUS PERMISSION
UNEXPECTED PERMISSION

android.permission.GET_ACCOUNTS

Allows access to the list of accounts in the Accounts Service.

DANGEROUS PERMISSION
UNEXPECTED PERMISSION

android.permission.GET_TASKS

This application can retrieve information about currently and recently running tasks. This may allow the app to discover information about other applications on the device.

DANGEROUS PERMISSION
UNEXPECTED PERMISSION

android.permission.MANAGE_ACCOUNTS

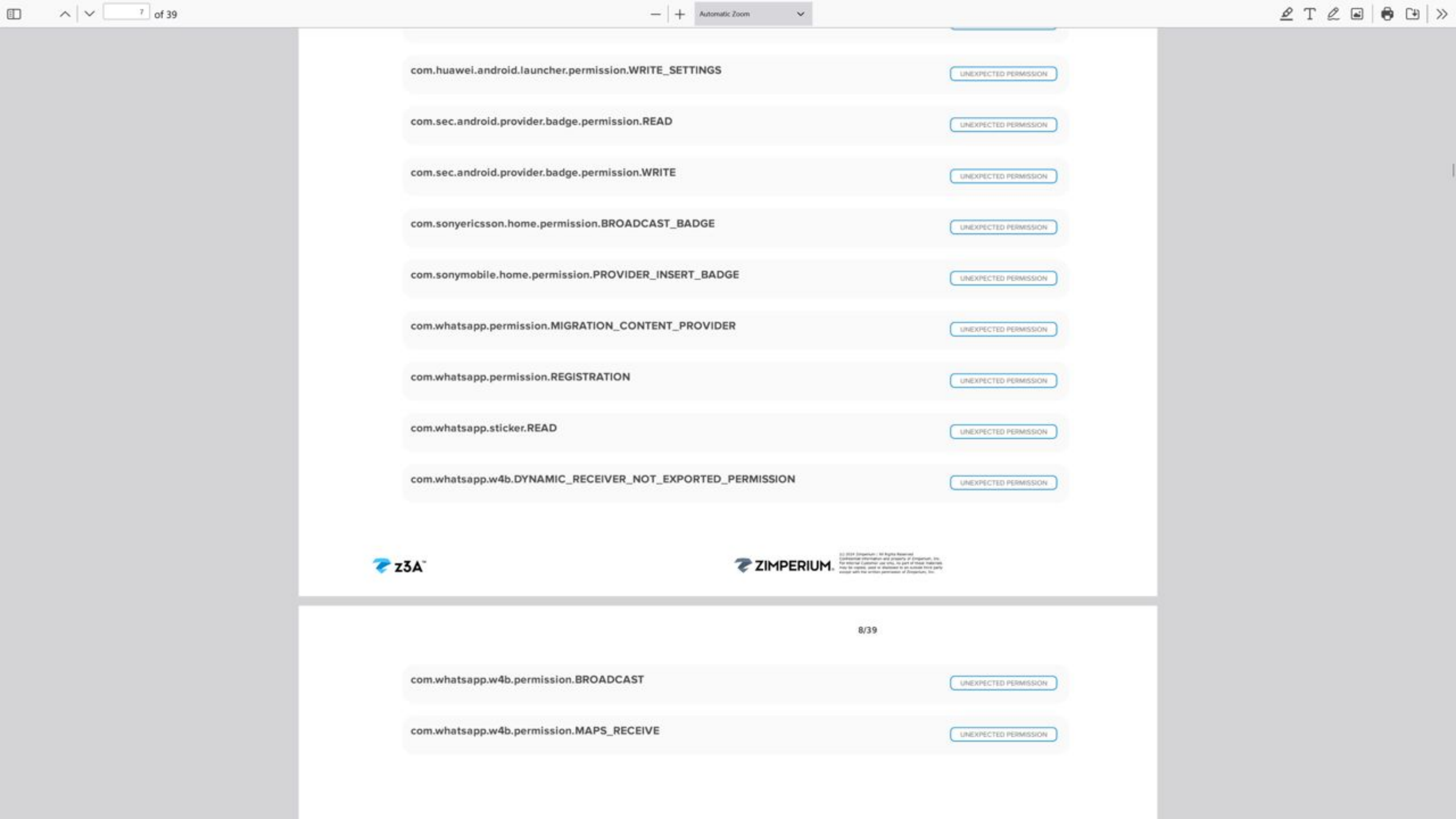
This application can perform operations like adding and removing accounts, and deleting their password.

DANGEROUS PERMISSION
UNEXPECTED PERMISSION

android.permission.MODIFY_AUDIO_SETTINGS

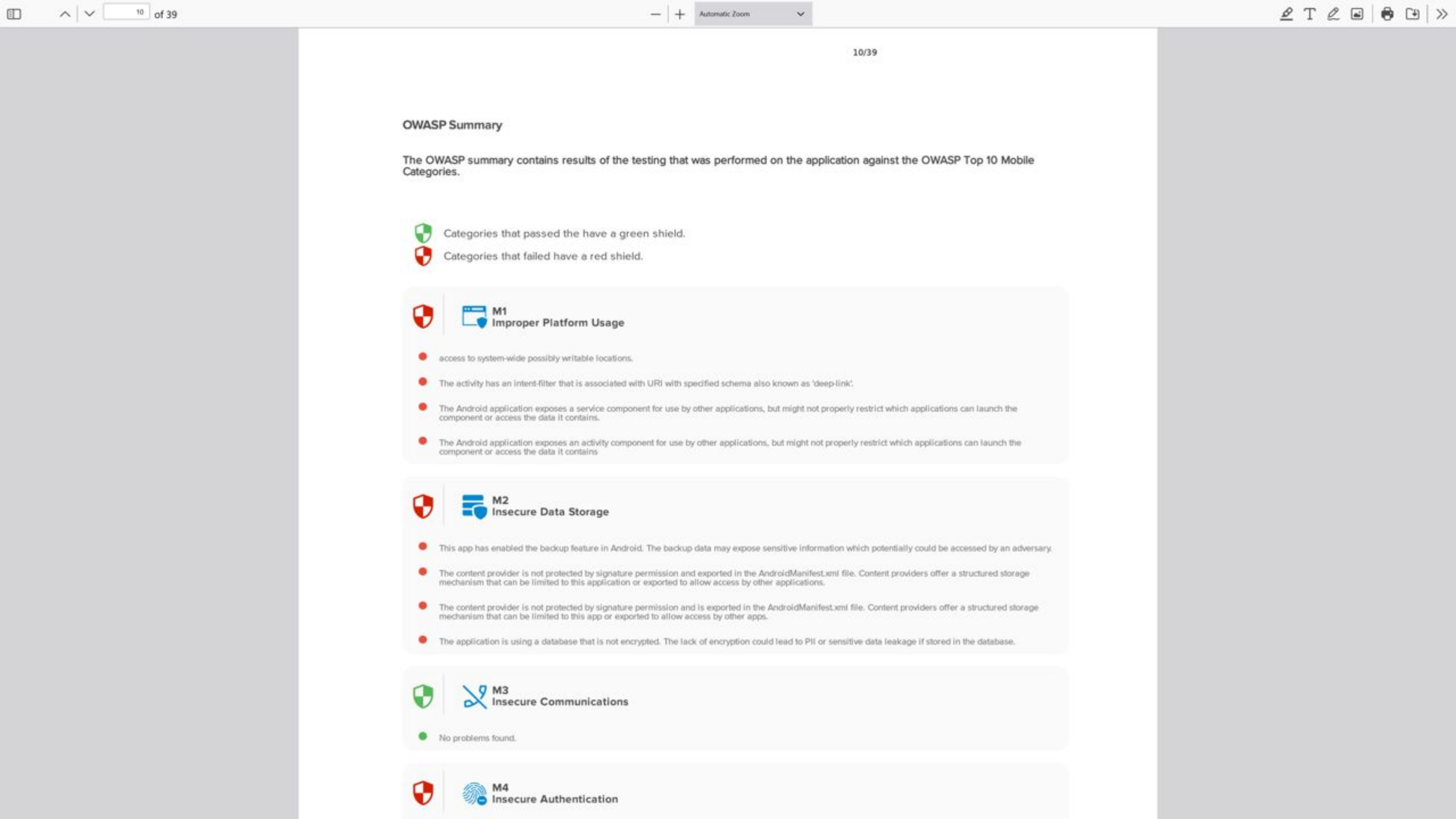
This application can control your audio settings such as volume levels.

DANGEROUS PERMISSION
UNEXPECTED PERMISSION



com.huawei.android.launcher.permission.WRITE_SETTINGS	UNEXPECTED PERMISSION
com.sec.android.provider.badge.permission.READ	UNEXPECTED PERMISSION
com.sec.android.provider.badge.permission.WRITE	UNEXPECTED PERMISSION
com.sonyericsson.home.permission.BROADCAST_BADGE	UNEXPECTED PERMISSION
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	UNEXPECTED PERMISSION
com.whatsapp.permission.MIGRATION_CONTENT_PROVIDER	UNEXPECTED PERMISSION
com.whatsapp.permission.REGISTRATION	UNEXPECTED PERMISSION
com.whatsapp.sticker.READ	UNEXPECTED PERMISSION
com.whatsapp.w4b.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	UNEXPECTED PERMISSION

com.whatsapp.w4b.permission.BROADCAST	UNEXPECTED PERMISSION
com.whatsapp.w4b.permission.MAPS_RECEIVE	UNEXPECTED PERMISSION



OWASP Summary

The OWASP summary contains results of the testing that was performed on the application against the OWASP Top 10 Mobile Categories.

Categories that passed the have a green shield.

Categories that failed have a red shield.

M1
Improper Platform Usage

- access to system-wide possibly writable locations.
- The activity has an intent-filter that is associated with URI with specified schema also known as 'deep-link'.
- The Android application exposes a service component for use by other applications, but might not properly restrict which applications can launch the component or access the data it contains.
- The Android application exposes an activity component for use by other applications, but might not properly restrict which applications can launch the component or access the data it contains

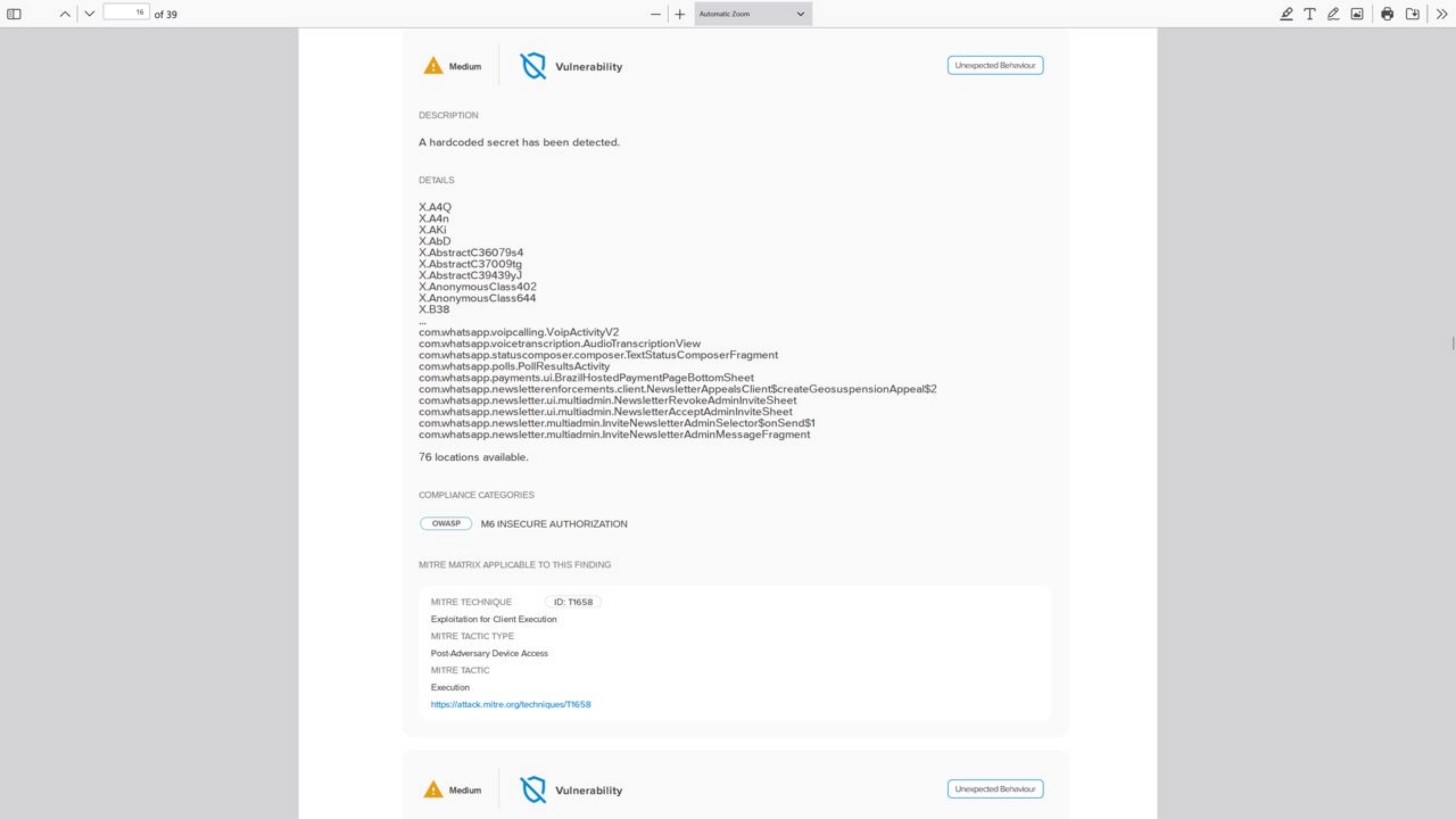
M2
Insecure Data Storage

- This app has enabled the backup feature in Android. The backup data may expose sensitive information which potentially could be accessed by an adversary.
- The content provider is not protected by signature permission and exported in the AndroidManifest.xml file. Content providers offer a structured storage mechanism that can be limited to this application or exported to allow access by other applications.
- 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.
- The application is using a database that is not encrypted. The lack of encryption could lead to PII or sensitive data leakage if stored in the database.

M3
Insecure Communications

- No problems found.

M4
Insecure Authentication



Medium

Vulnerability

Unexpected Behaviour

DESCRIPTION

A hardcoded secret has been detected.

DETAILS

```
X.A4Q
X.A4n
X.AKi
X.AbD
X.AbstractC36079s4
X.AbstractC37009tg
X.AbstractC39439yJ
X.AnonymousClass402
X.AnonymousClass644
X.B38
...
com.whatsapp.voipcalling.VoipActivityV2
com.whatsapp.voicetranscription.AudioTranscriptionView
com.whatsapp.statuscomposer.composer.TextStatusComposerFragment
com.whatsapp.polls.PollResultsActivity
com.whatsapp.payments.ui.BrazilHostedPaymentPageBottomSheet
com.whatsapp.newsletterenforcements.client.NewsletterAppealsClient$createGeosuspensionAppeal$2
com.whatsapp.newsletter.ui.multiadmin.NewsletterRevokeAdminInviteSheet
com.whatsapp.newsletter.ui.multiadmin.NewsletterAcceptAdminInviteSheet
com.whatsapp.newsletter.multiadmin.InviteNewsletterAdminSelector$onSend$1
com.whatsapp.newsletter.multiadmin.InviteNewsletterAdminMessageFragment
```

76 locations available.

COMPLIANCE CATEGORIES

OWASP M6 INSECURE AUTHORIZATION

MITRE MATRIX APPLICABLE TO THIS FINDING

MITRE TECHNIQUE ID: T1658

Exploitation for Client Execution

MITRE TACTIC TYPE

Post-Adversary Device Access

MITRE TACTIC

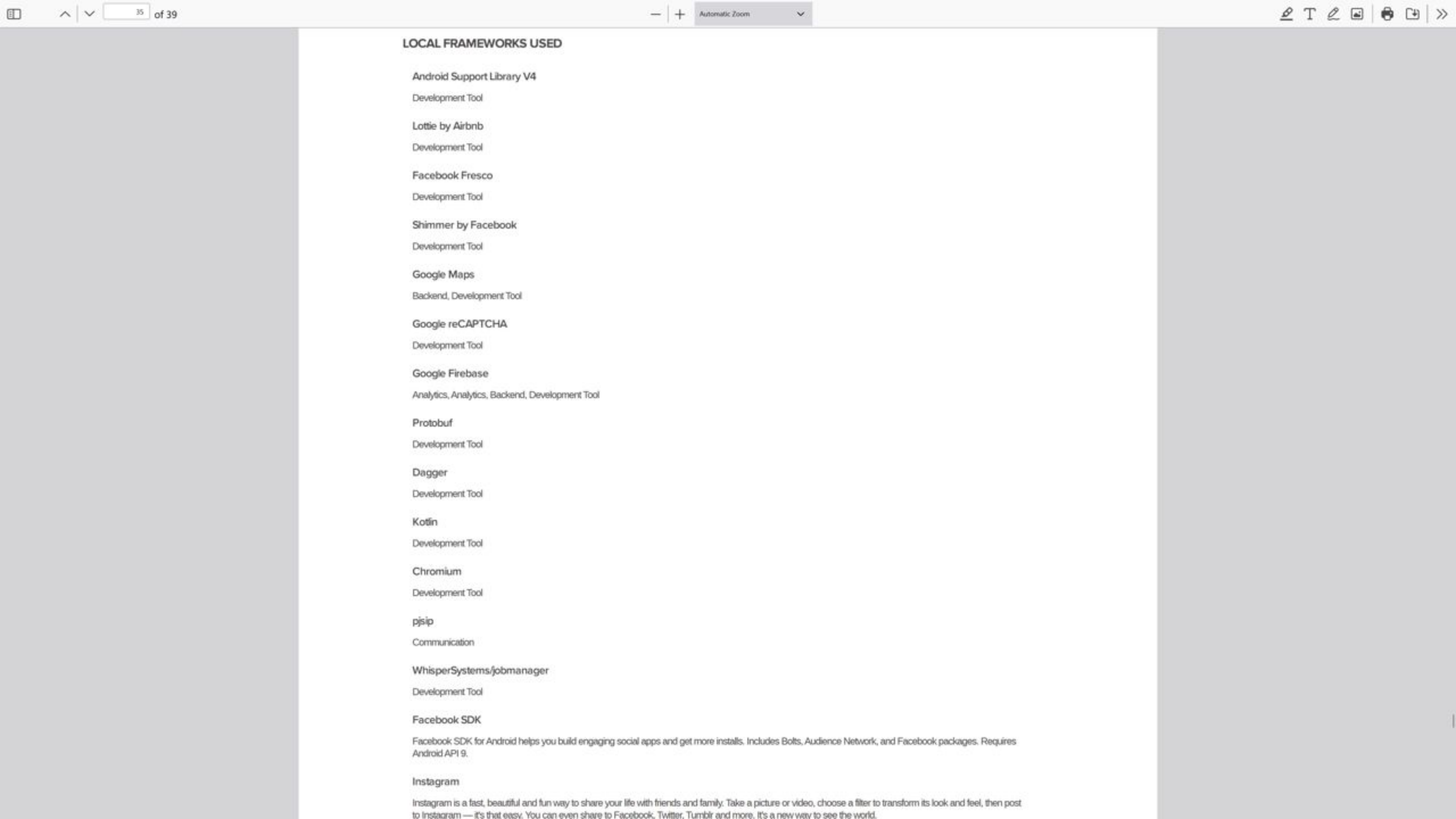
Execution

https://attack.mitre.org/techniques/T1658

Medium

Vulnerability

Unexpected Behaviour



LOCAL FRAMEWORKS USED

Android Support Library V4

Development Tool

Lottie by Airbnb

Development Tool

Facebook Fresco

Development Tool

Shimmer by Facebook

Development Tool

Google Maps

Backend, Development Tool

Google reCAPTCHA

Development Tool

Google Firebase

Analytics, Analytics, Backend, Development Tool

Protobuf

Development Tool

Dagger

Development Tool

Kotlin

Development Tool

Chromium

Development Tool

pjsip

Communication

WhisperSystems/jobmanager

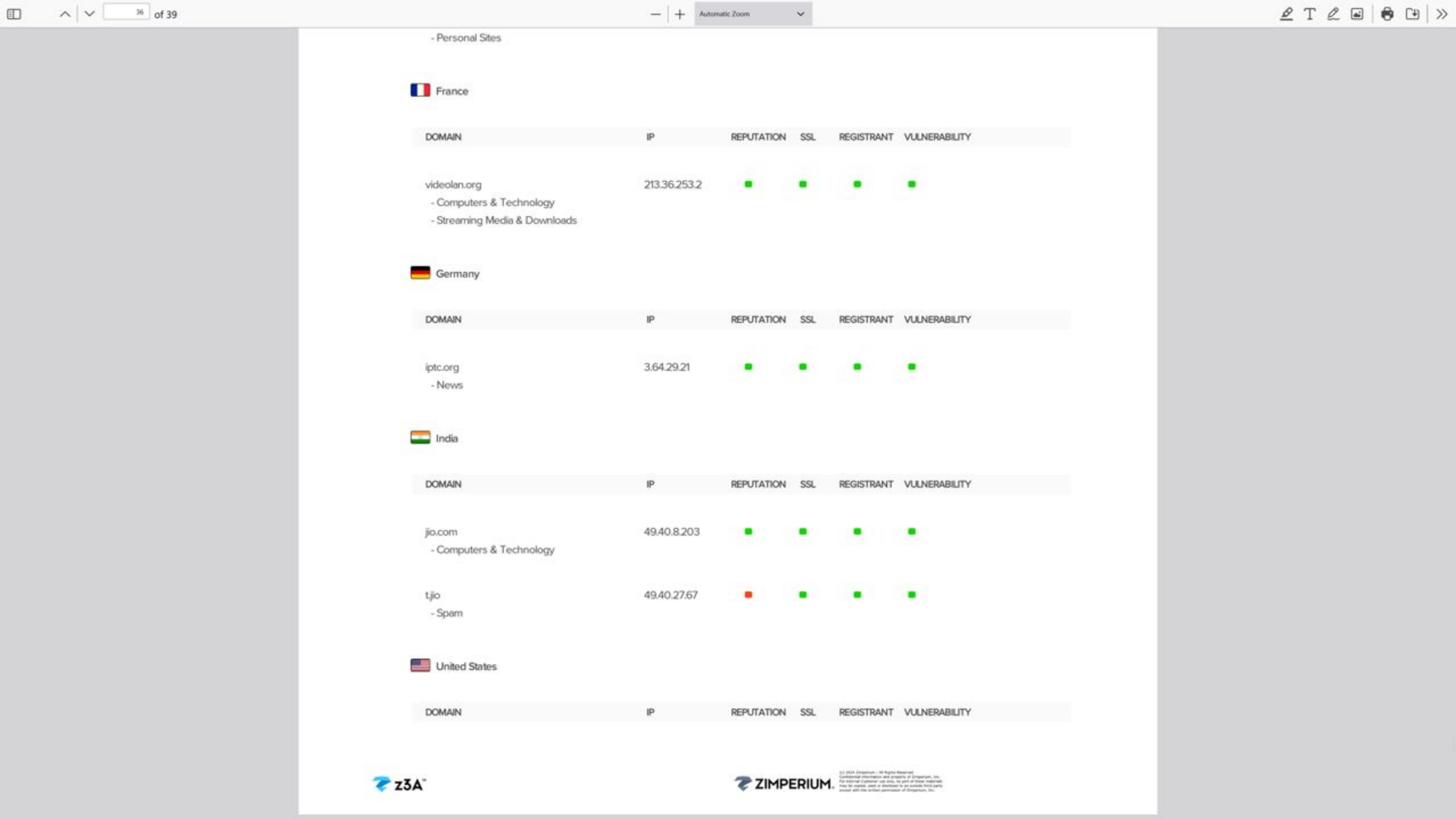
Development Tool

Facebook SDK

Facebook SDK for Android helps you build engaging social apps and get more installs. Includes Bolts, Audience Network, and Facebook packages. Requires Android API 9.

Instagram

Instagram is a fast, beautiful and fun way to share your life with friends and family. Take a picture or video, choose a filter to transform its look and feel, then post to Instagram — it's that easy. You can even share to Facebook, Twitter, Tumblr and more. It's a new way to see the world.



- Personal Sites

France

DOMAIN	IP	REPUTATION	SSL	REGISTRANT	VULNERABILITY
videolan.org - Computers & Technology - Streaming Media & Downloads	213.36.253.2	🟩	🟩	🟩	🟩

Germany

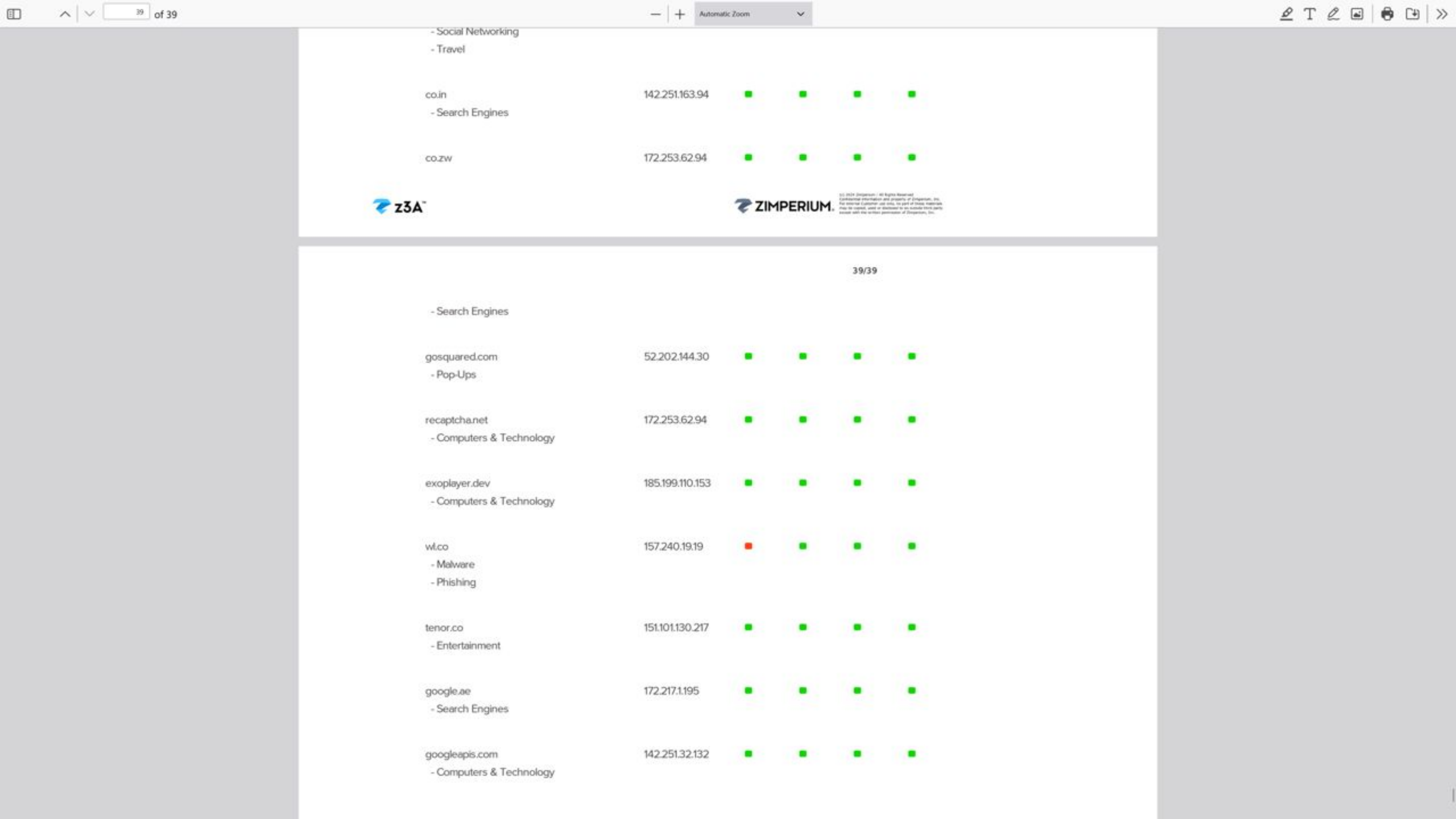
DOMAIN	IP	REPUTATION	SSL	REGISTRANT	VULNERABILITY
iptc.org - News	3.64.29.21	🟩	🟩	🟩	🟩

India

DOMAIN	IP	REPUTATION	SSL	REGISTRANT	VULNERABILITY
jio.com - Computers & Technology	49.40.8.203	🟩	🟩	🟩	🟩
t.jio - Spam	49.40.27.67	🟥	🟩	🟩	🟩

United States

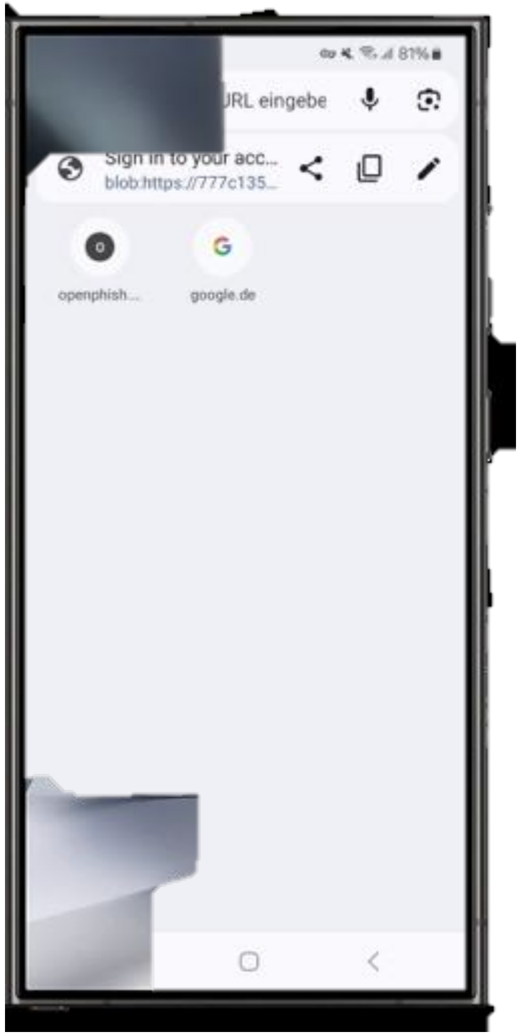
DOMAIN	IP	REPUTATION	SSL	REGISTRANT	VULNERABILITY



- Social Networking - Travel					
co.in - Search Engines	142.251.163.94	🟩	🟩	🟩	🟩
co.zw	172.253.62.94	🟩	🟩	🟩	🟩

- Search Engines					
gosquared.com - Pop-Ups	52.202.144.30	🟩	🟩	🟩	🟩
recaptcha.net - Computers & Technology	172.253.62.94	🟩	🟩	🟩	🟩
exoplayer.dev - Computers & Technology	185.199.110.153	🟩	🟩	🟩	🟩
wl.co - Malware - Phishing	157.240.19.19	🟥	🟩	🟩	🟩
tenor.co - Entertainment	151.101.130.217	🟩	🟩	🟩	🟩
google.ae - Search Engines	172.217.1.195	🟩	🟩	🟩	🟩
googleapis.com - Computers & Technology	142.251.32.132	🟩	🟩	🟩	🟩

Threat exposure for mobile devices



81%

URL eingebe

Sign in to your acc...
blob:https://777c135...

https://bit.ly/45nIn1Z

Device

65% *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

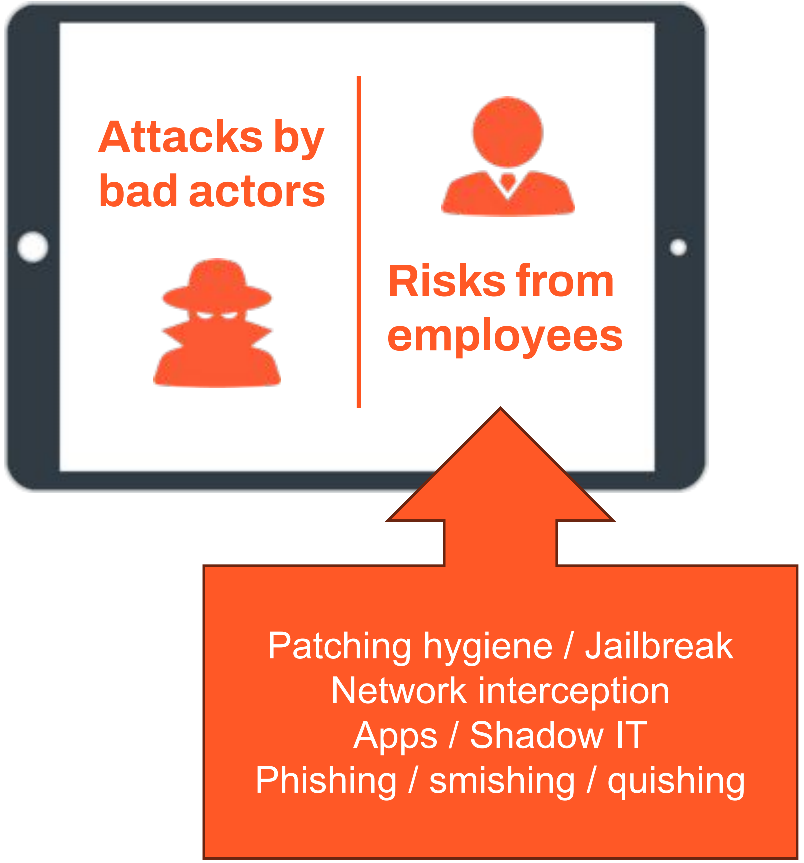
New mobile malware signatures per month

Phishing

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

Threat exposure for mobile devices

CYBER HYGIENE



Attacks by bad actors

Risks from employees

Patching hygiene / Jailbreak
Network interception
Apps / Shadow IT
Phishing / smishing / quishing

Device

65% *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 signatures per month

Phishing

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

Demo scenario

- Making it hard for the user.... **PDF** files and **phishing**

- Making life easier... but riskier... **Shortcuts**

- User **jailbreaks** devices
- ... regrets it and tries to hide it
- ... but we have forensic analysis

- Give the user the tools to increase its mobile cyber hygiene
- ... stop links
- ... **QR code scanner**

Recommended Next Steps

SCAN ME

✓

Understand why mobile cyber hygiene is key

Vet your Mobile App

Receive a personalized app analysis of YOUR mobile app or a mobile app of your choice

✓

Test For Yourself

Pilot the solution internally to validate enterprise fit

a Mobile-First Security Strategy

C

1. **Prioritize risk at the edge:** secure the mobile-powered business reality, across all devices and apps, any platform

2. **Operate in a known state:** complete visibility of your mobile ecosystem and risk level, automatically assess vulnerabilities, never throttle productivity - measurable, auditable and insurable

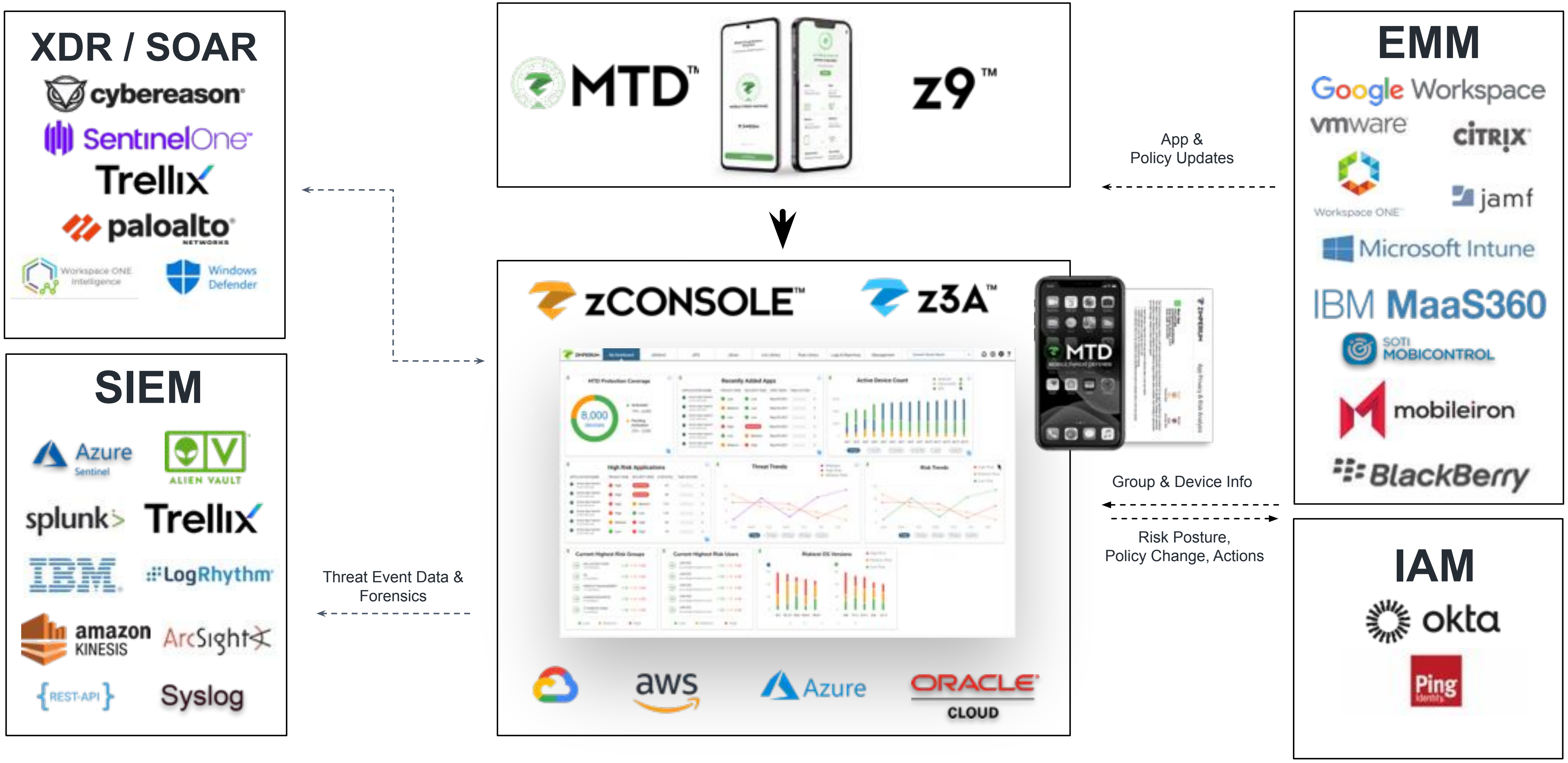
3. **Step-up detection and response:** detect and prioritize anomalies, contextual threat response, resolve vulnerabilities and incidents proactively, embed security across device and application lifecycle for tamper-proof/threat-aware mobile experiences

4. **Start the autonomous journey:** dynamically respond to threats and ever-changing mobile ecosystem, automatically isolate compromised devices/ untrusted environments, scale a proactive security posture, build resilience

5. **Never break the law:** govern compliance, stay ahead of global regulations, data sovereignty, and privacy regulations while respecting work/life boundaries

Architecture and Trellix integrations

MTD™ Platform Ecosystem



XDR / SOAR

cybereason

SentinelOne

Trellix

paloalto NETWORKS

Workspace ONE Intelligence

Windows Defender

SIEM

Azure Sentinel

ALIEN VAULT

splunk>

Trellix

IBM

LogRhythm

amazon KINESIS

ArcSight

{REST-API}

Syslog

MTD™

z9™

zCONSOLE™

z3A™

MTD

Google Cloud

aws

Azure

ORACLE CLOUD

Threat Event Data & Forensics

App & Policy Updates

Group & Device Info

Risk Posture, Policy Change, Actions

EMM

Google Workspace

vmware

CiTRIX

Workspace ONE

jamf

Microsoft Intune

IBM MaaS360

SOTI MOBICONTROL

mobileiron

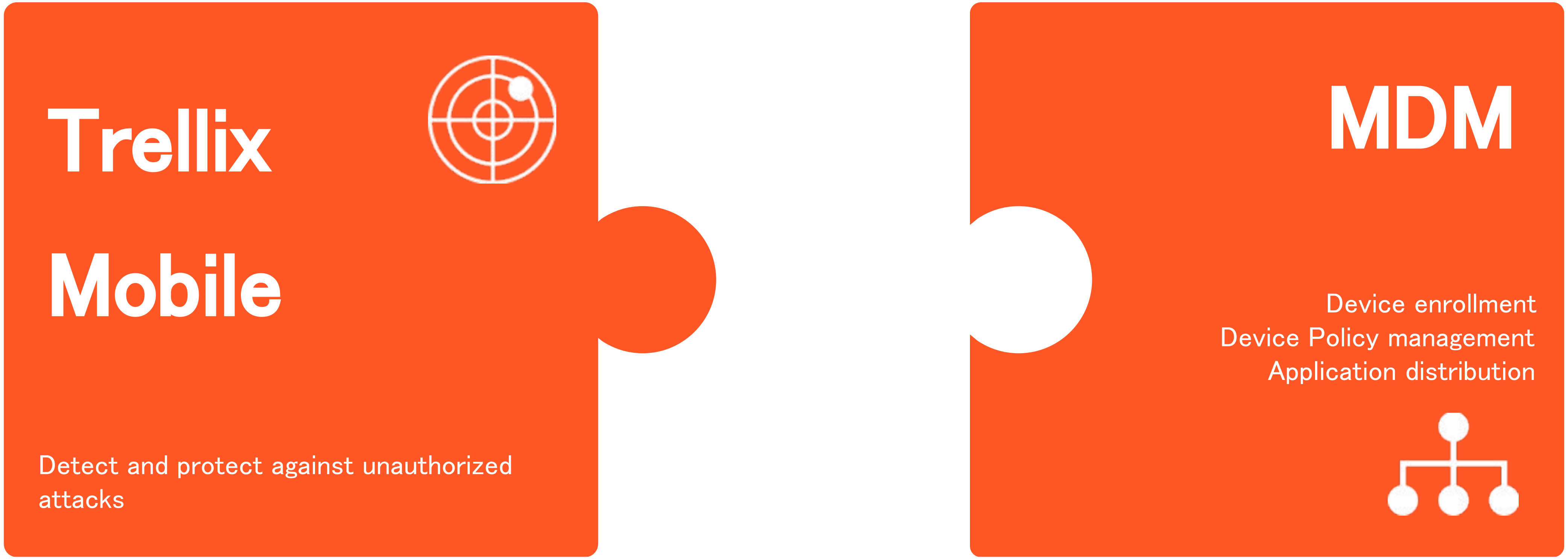
BlackBerry

IAM

okta

Ping Identity

MDM+Trellix Mobile = Best protection together



Trellix

Mobile

Detect and protect against unauthorized attacks

MDM

Device enrollment
Device Policy management
Application distribution

BlackBerry UEM

Business Concierge

Citrix

IBM MaaS360

JAMF Pro

Microsoft

Microsoft

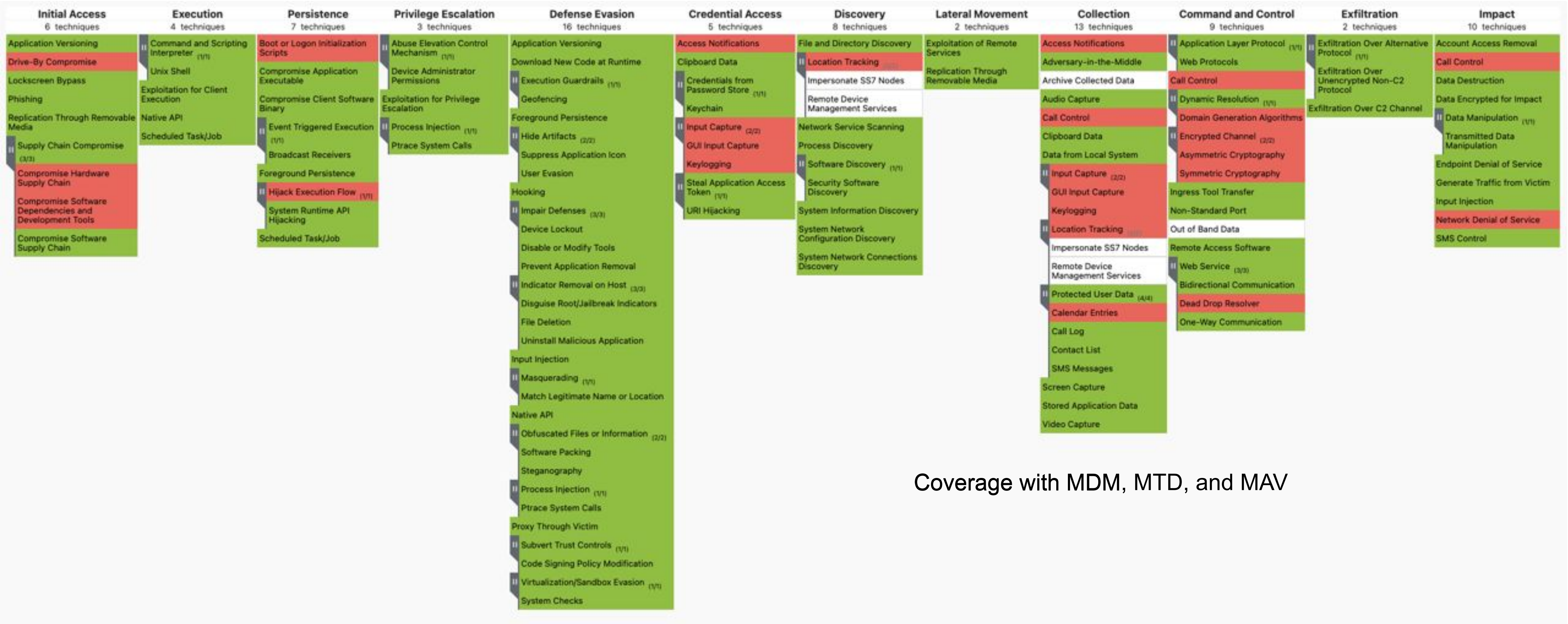
MobileIron Cloud

MobileIron Core

SOTI MobiControl

VMware Workspace ONE UEM

MITRE ATT&CK Coverage



Initial Access
6 techniques

- 🟩 Application Versioning
- 🟥 Drive-By Compromise
- 🟩 Lockscreen Bypass
- 🟩 Phishing
- 🟩 Replication Through Removable Media
- 🟩 Supply Chain Compromise (3/3)
  - 🟥 Compromise Hardware Supply Chain
  - 🟥 Compromise Software Dependencies and Development Tools
  - 🟩 Compromise Software Supply Chain

Execution
4 techniques

- 🟩 Command and Scripting Interpreter (1/1)
  - 🟩 Unix Shell
- 🟩 Exploitation for Client Execution
- 🟩 Native API
- 🟩 Scheduled Task/Job

Persistence
7 techniques

- 🟥 Boot or Logon Initialization Scripts
- 🟩 Compromise Application Executable
- 🟩 Compromise Client Software Binary
- 🟩 Event Triggered Execution (1/1)
  - 🟩 Broadcast Receivers
- 🟩 Foreground Persistence
- 🟥 Hijack Execution Flow (1/1)
  - 🟩 System Runtime API Hijacking
- 🟩 Scheduled Task/Job

Privilege Escalation
3 techniques

- 🟩 Abuse Elevation Control Mechanism (1/1)
  - 🟩 Device Administrator Permissions
- 🟩 Exploitation for Privilege Escalation
- 🟩 Process Injection (1/1)
  - 🟩 Ptrace System Calls

Defense Evasion
16 techniques

- 🟩 Application Versioning
- 🟩 Download New Code at Runtime
- 🟩 Execution Guardrails (1/1)
  - 🟩 Geofencing
- 🟩 Foreground Persistence
- 🟩 Hide Artifacts (2/2)
  - 🟩 Suppress Application Icon
  - 🟩 User Evasion
- 🟩 Hooking
- 🟩 Impair Defenses (3/3)
  - 🟩 Device Lockout
  - 🟩 Disable or Modify Tools
  - 🟩 Prevent Application Removal
- 🟩 Indicator Removal on Host (3/3)
  - 🟩 Disguise Root/Jailbreak Indicators
  - 🟩 File Deletion
  - 🟩 Uninstall Malicious Application
- 🟩 Input Injection
- 🟩 Masquerading (1/1)
  - 🟩 Match Legitimate Name or Location
- 🟩 Native API
- 🟩 Obfuscated Files or Information (2/2)
  - 🟩 Software Packing
  - 🟩 Steganography
- 🟩 Process Injection (1/1)
  - 🟩 Ptrace System Calls
- 🟩 Proxy Through Victim
- 🟩 Subvert Trust Controls (1/1)
  - 🟩 Code Signing Policy Modification
- 🟩 Virtualization/Sandbox Evasion (1/1)
  - 🟩 System Checks

Credential Access
5 techniques

- 🟥 Access Notifications
- 🟩 Clipboard Data
- 🟩 Credentials from Password Store (1/1)
  - 🟩 Keychain
- 🟥 Input Capture (2/2)
  - 🟥 GUI Input Capture
  - 🟥 Keylogging
- 🟩 Steal Application Access Token (1/1)
  - 🟩 URI Hijacking

Discovery
8 techniques

- 🟩 File and Directory Discovery
- 🟥 Location Tracking
  - ⬜ Impersonate SS7 Nodes
  - ⬜ Remote Device Management Services
- 🟩 Network Service Scanning
- 🟩 Process Discovery
- 🟩 Software Discovery (1/1)
  - 🟩 Security Software Discovery
- 🟩 System Information Discovery
- 🟩 System Network Configuration Discovery
- 🟩 System Network Connections Discovery

Lateral Movement
2 techniques

- 🟩 Exploitation of Remote Services
- 🟩 Replication Through Removable Media

Collection
13 techniques

- 🟥 Access Notifications
- 🟩 Adversary-in-the-Middle
- ⬜ Archive Collected Data
- 🟩 Audio Capture
- 🟥 Call Control
- 🟩 Clipboard Data
- 🟩 Data from Local System
- 🟥 Input Capture (2/2)
  - 🟥 GUI Input Capture
  - 🟥 Keylogging
- 🟥 Location Tracking
  - ⬜ Impersonate SS7 Nodes
  - ⬜ Remote Device Management Services
- 🟩 Protected User Data (4/4)
  - 🟥 Calendar Entries
  - 🟩 Call Log
  - 🟩 Contact List
  - 🟩 SMS Messages
- 🟩 Screen Capture
- 🟩 Stored Application Data
- 🟩 Video Capture

Command and Control
9 techniques

- 🟩 Application Layer Protocol (1/1)
  - 🟩 Web Protocols
- 🟥 Call Control
- 🟩 Dynamic Resolution (1/1)
  - 🟥 Domain Generation Algorithms
- 🟥 Encrypted Channel (2/2)
  - 🟥 Asymmetric Cryptography
  - 🟥 Symmetric Cryptography
- 🟩 Ingress Tool Transfer
- 🟩 Non-Standard Port
- ⬜ Out of Band Data
- 🟩 Remote Access Software
- 🟩 Web Service (3/3)
  - 🟩 Bidirectional Communication
  - 🟥 Dead Drop Resolver
  - 🟩 One-Way Communication

Exfiltration
2 techniques

- 🟩 Exfiltration Over Alternative Protocol (1/1)
  - 🟩 Exfiltration Over Unencrypted Non-C2 Protocol
- 🟩 Exfiltration Over C2 Channel

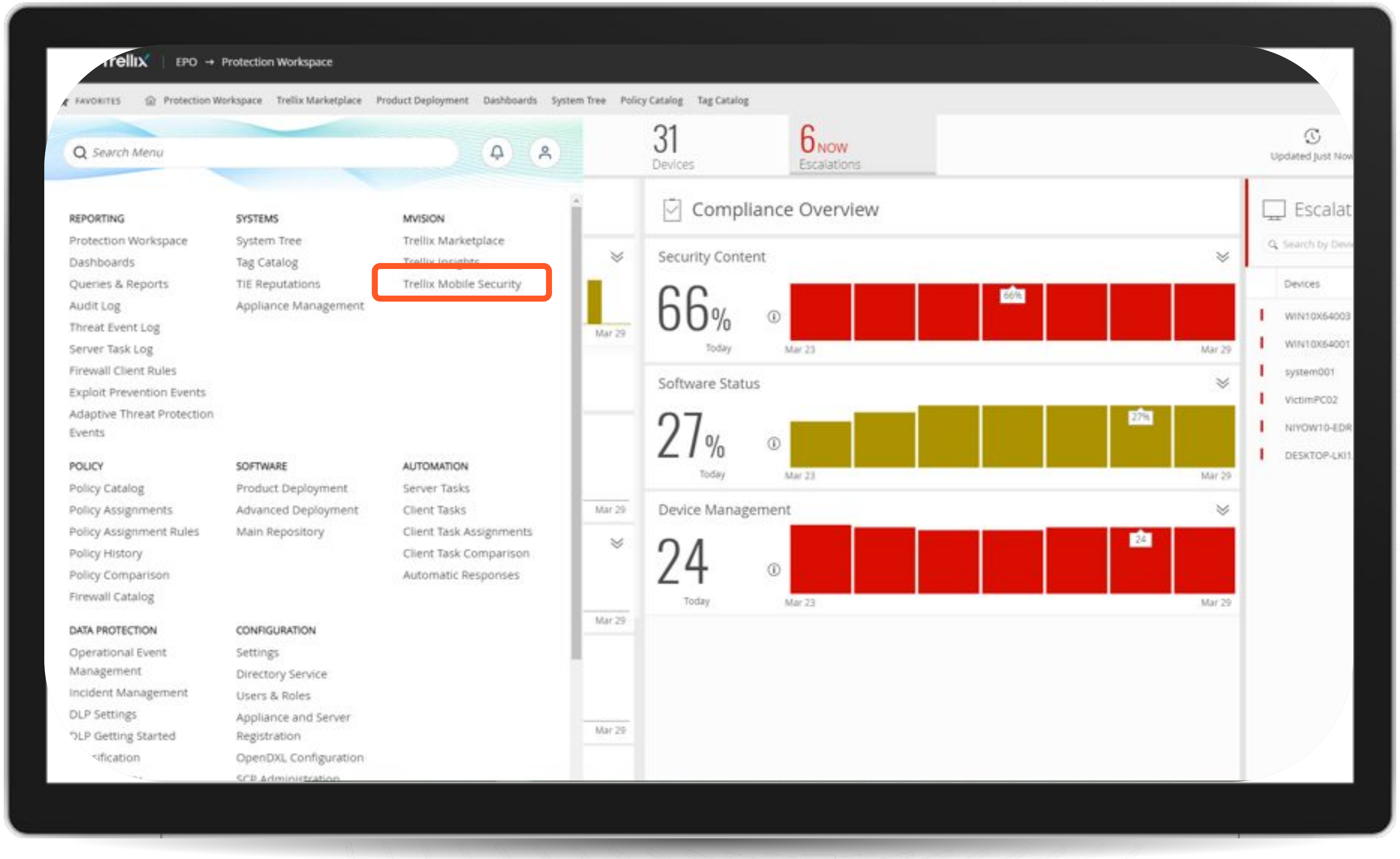
Impact
10 techniques

- 🟩 Account Access Removal
- 🟥 Call Control
- 🟩 Data Destruction
- 🟩 Data Encrypted for Impact
- 🟩 Data Manipulation (1/1)
  - 🟩 Transmitted Data Manipulation
- 🟩 Endpoint Denial of Service
- 🟩 Generate Traffic from Victim
- 🟩 Input Injection
- 🟥 Network Denial of Service
- 🟩 SMS Control

Coverage with MDM, MTD, and MAV

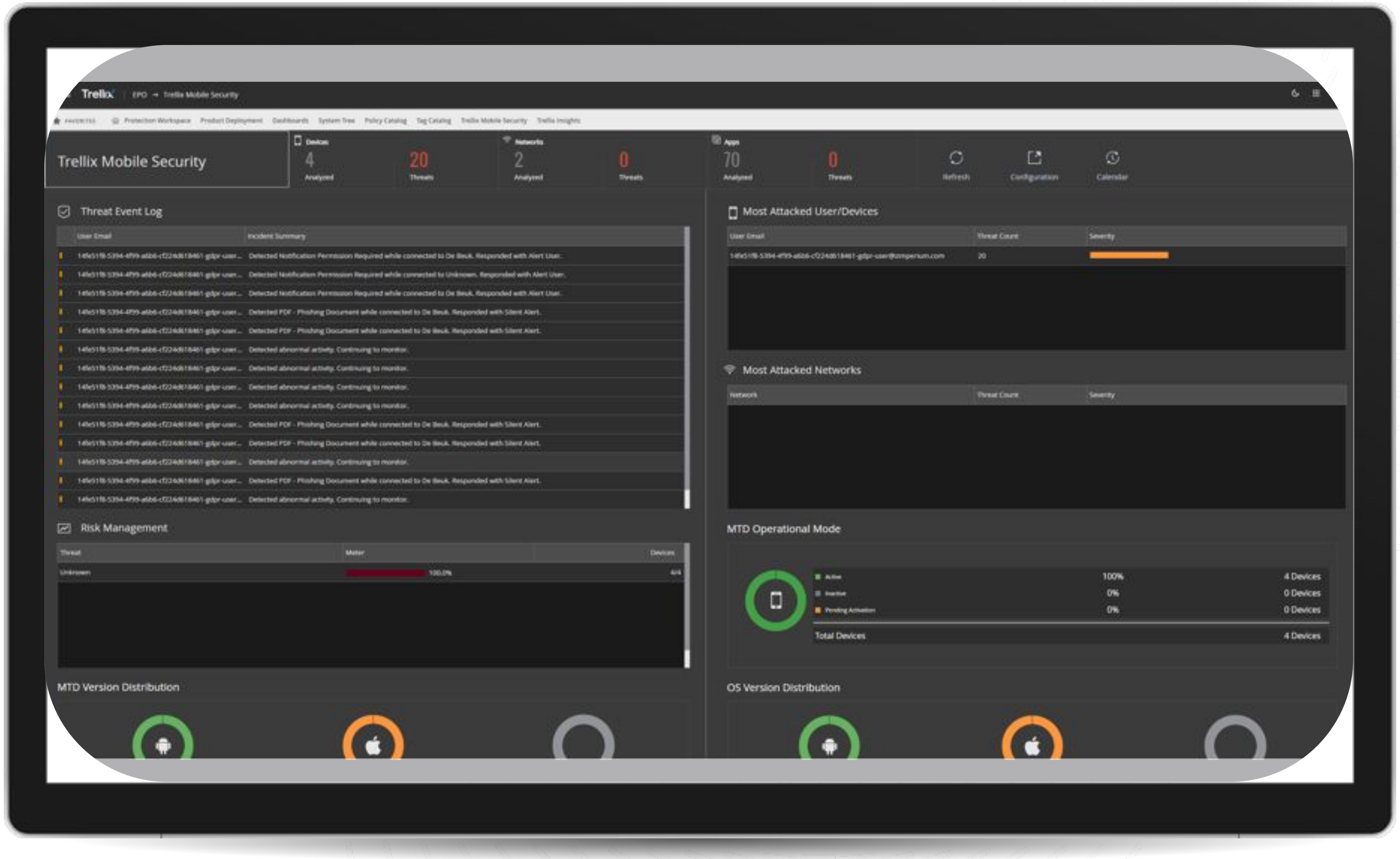
How do we manage?

Direct access - No Configuration
Click and Access to the Tenant



Trellix ZIMPERIUM

Direct access - No Configuration
Click and Access to the Tenant



Trellix Mobile Security

Devices		Networks		Apps	
4	20	2	0	70	0
Analyzed	Threats	Analyzed	Threats	Analyzed	Threats

Threat Event Log

User Email	Incident Summary
14fe51f8-5394-4f99-a6b6-cf224d618461-gdpr-user...	Detected Notification Permission Required while connected to De Beuk. Responded with Alert User.
14fe51f8-5394-4f99-a6b6-cf224d618461-gdpr-user...	Detected Notification Permission Required while connected to Unknown. Responded with Alert User.
14fe51f8-5394-4f99-a6b6-cf224d618461-gdpr-user...	Detected Notification Permission Required while connected to De Beuk. Responded with Alert User.
14fe51f8-5394-4f99-a6b6-cf224d618461-gdpr-user...	Detected PDF - Phishing Document while connected to De Beuk. Responded with Silent Alert.
14fe51f8-5394-4f99-a6b6-cf224d618461-gdpr-user...	Detected PDF - Phishing Document while connected to De Beuk. Responded with Silent Alert.
14fe51f8-5394-4f99-a6b6-cf224d618461-gdpr-user...	Detected abnormal activity. Continuing to monitor.
14fe51f8-5394-4f99-a6b6-cf224d618461-gdpr-user...	Detected abnormal activity. Continuing to monitor.
14fe51f8-5394-4f99-a6b6-cf224d618461-gdpr-user...	Detected abnormal activity. Continuing to monitor.
14fe51f8-5394-4f99-a6b6-cf224d618461-gdpr-user...	Detected abnormal activity. Continuing to monitor.
14fe51f8-5394-4f99-a6b6-cf224d618461-gdpr-user...	Detected PDF - Phishing Document while connected to De Beuk. Responded with Silent Alert.
14fe51f8-5394-4f99-a6b6-cf224d618461-gdpr-user...	Detected PDF - Phishing Document while connected to De Beuk. Responded with Silent Alert.
14fe51f8-5394-4f99-a6b6-cf224d618461-gdpr-user...	Detected abnormal activity. Continuing to monitor.
14fe51f8-5394-4f99-a6b6-cf224d618461-gdpr-user...	Detected PDF - Phishing Document while connected to De Beuk. Responded with Silent Alert.
14fe51f8-5394-4f99-a6b6-cf224d618461-gdpr-user...	Detected abnormal activity. Continuing to monitor.

Most Attacked User/Devices

User Email	Threat Count	Severity
14fe51f8-5394-4f99-a6b6-cf224d618461-gdpr-user@zimperium.com	20	🟧

Most Attacked Networks

Network	Threat Count	Severity

Risk Management

Threat	Meter	Devices
Unknown	100.0%	4/4

MTD Operational Mode

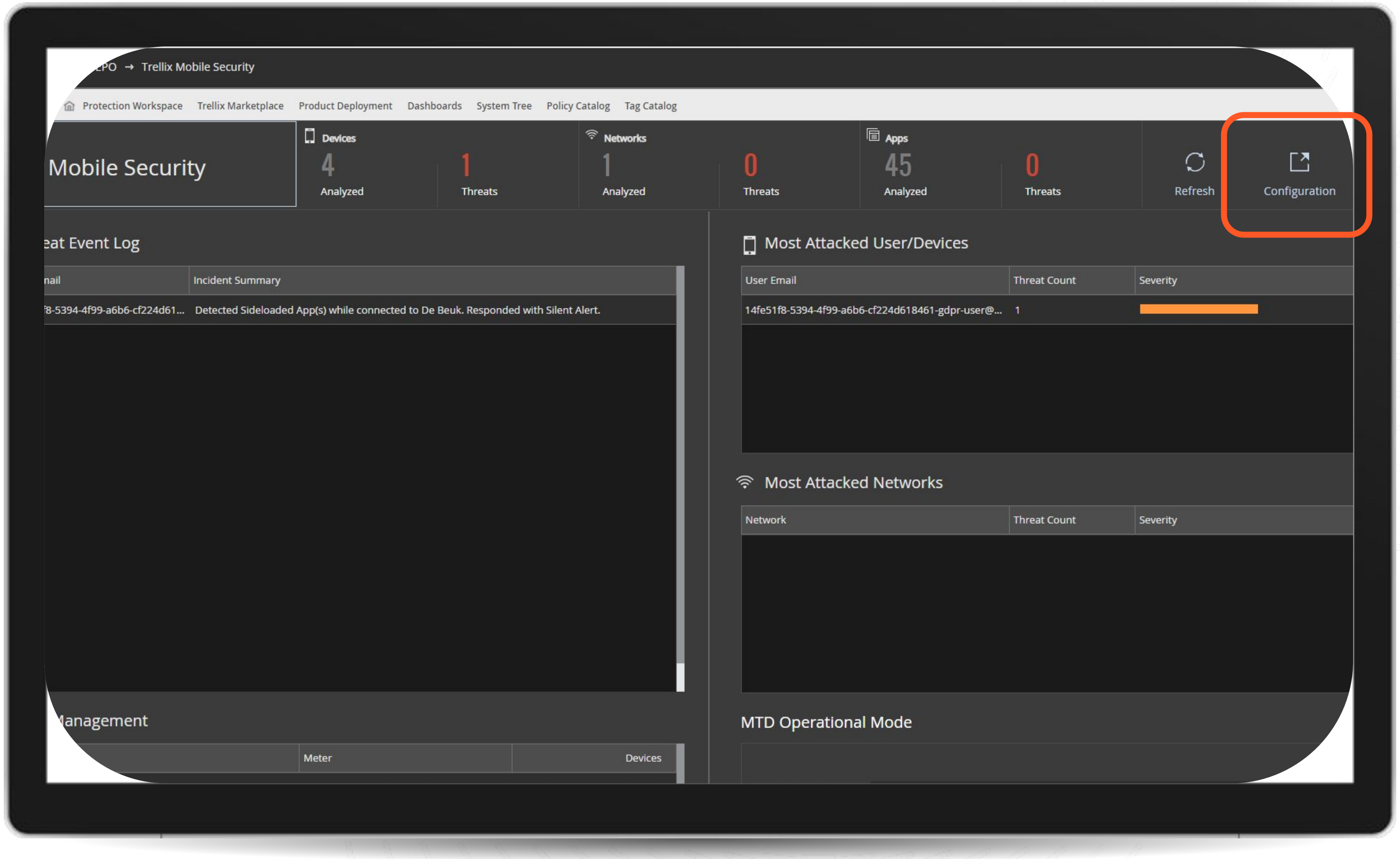
🟩 Active	100%	4 Devices
⬜ Inactive	0%	0 Devices
🟧 Pending Activation	0%	0 Devices
Total Devices		4 Devices

MTD Version Distribution

OS Version Distribution

Trellix ZIMPERIUM.

Tenant configuration



EPO → Trellix Mobile Security

Protection Workspace | Trellix Marketplace | Product Deployment | Dashboards | System Tree | Policy Catalog | Tag Catalog

Mobile Security

Devices		Networks		Apps	
4 Analyzed	1 Threats	1 Analyzed	0 Threats	45 Analyzed	0 Threats

eat Event Log

nail	Incident Summary
f8-5394-4f99-a6b6-cf224d61...	Detected Sideloaded App(s) while connected to De Beuk. Responded with Silent Alert.

Most Attacked User/Devices

User Email	Threat Count	Severity
14fe51f8-5394-4f99-a6b6-cf224d618461-gdpr-user@...	1	

Most Attacked Networks

Network	Threat Count	Severity

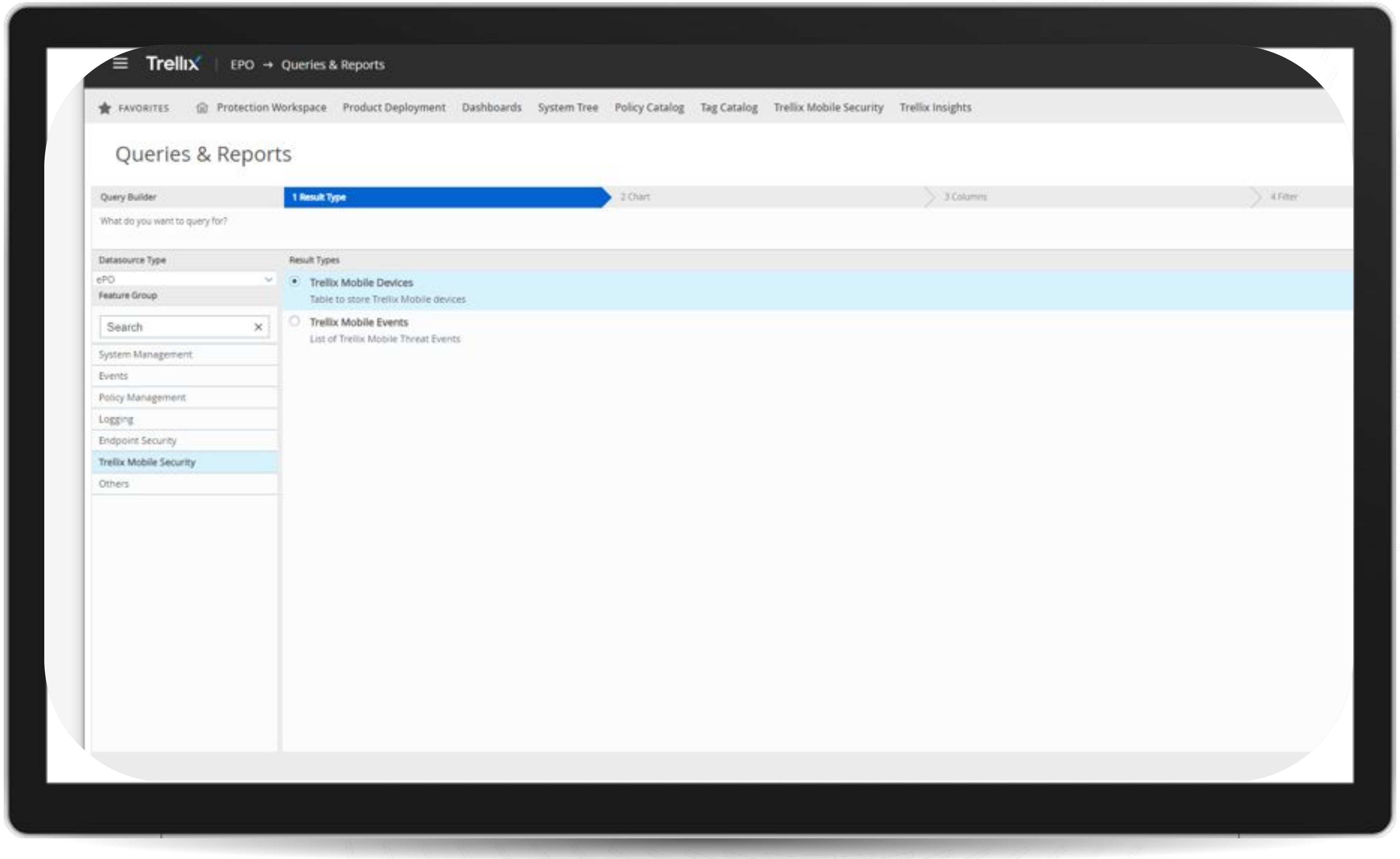
lanagement

	Meter	Devices

MTD Operational Mode

Trellix ZIMPERIUM.

Direct access - No Configuration
Click and Access to the Tenant



Trellix | EPO → Queries & Reports

★ FAVORITES | Protection Workspace | Product Deployment | Dashboards | System Tree | Policy Catalog | Tag Catalog | Trellix Mobile Security | Trellix Insights

Queries & Reports

Query Builder | 1 Result Type | 2 Chart | 3 Columns | 4 Filter

What do you want to query for?

Datasource Type: ePO

Feature Group

Search ✕

- System Management
- Events
- Policy Management
- Logging
- Endpoint Security
- Trellix Mobile Security
- Others

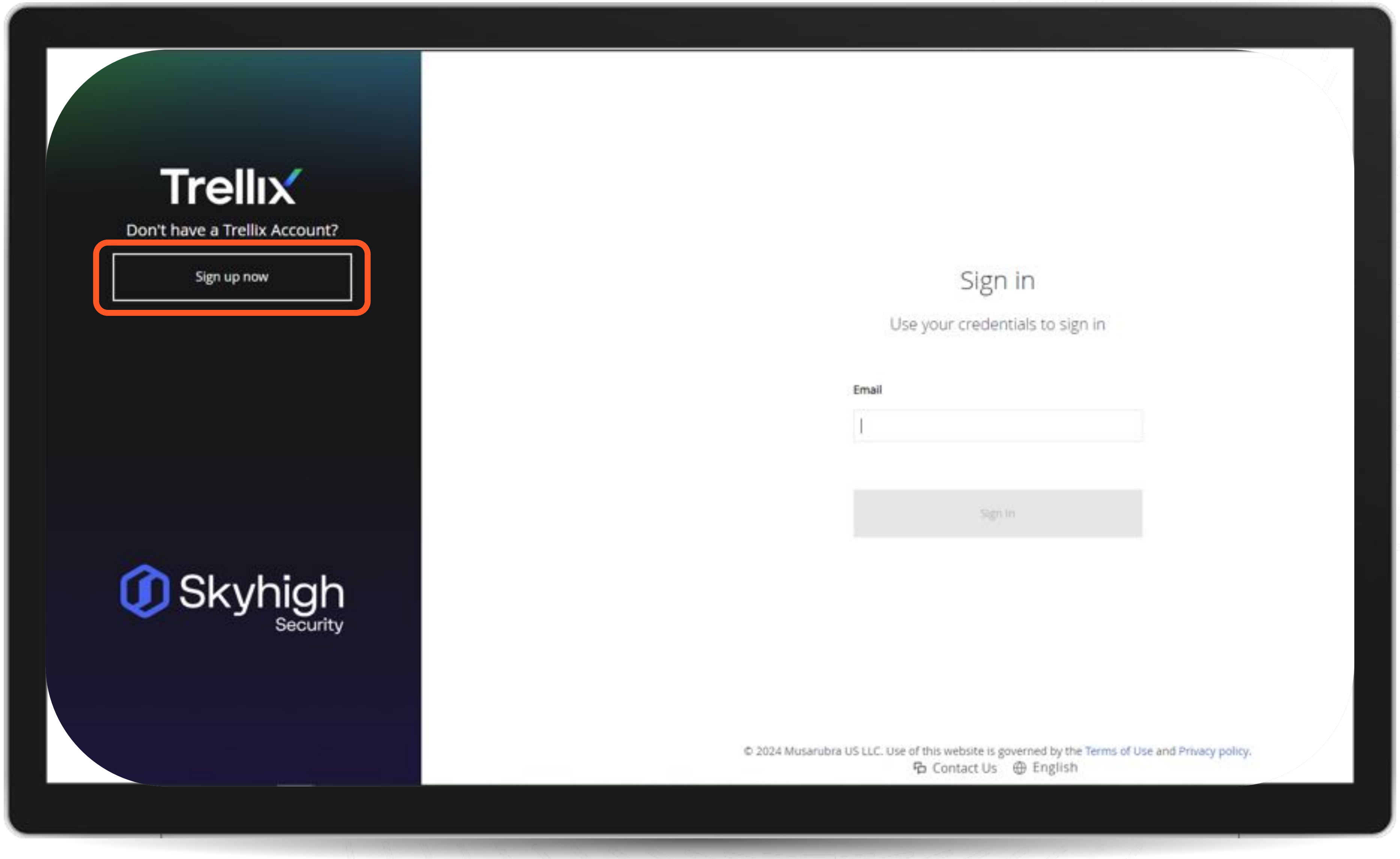
Result Types

● Trellix Mobile Devices
Table to store Trellix Mobile devices

○ Trellix Mobile Events
List of Trellix Mobile Threat Events

Trellix ZIMPERIUM.

Request your tenant at https://xconsole.trellix.com/



Don't have a Trellix Account?

Sign in

Use your credentials to sign in

Email

© 2024 Musarubra US LLC. Use of this website is governed by the Terms of Use and Privacy policy.

Recommended
Next Steps

SCAN ME

✓

Understand why mobile cyber hygiene is key

Vet your Mobile App

Receive a personalized app analysis of YOUR mobile app or a mobile app of your choice

✓

Test For Yourself

Pilot the solution internally to validate enterprise fit