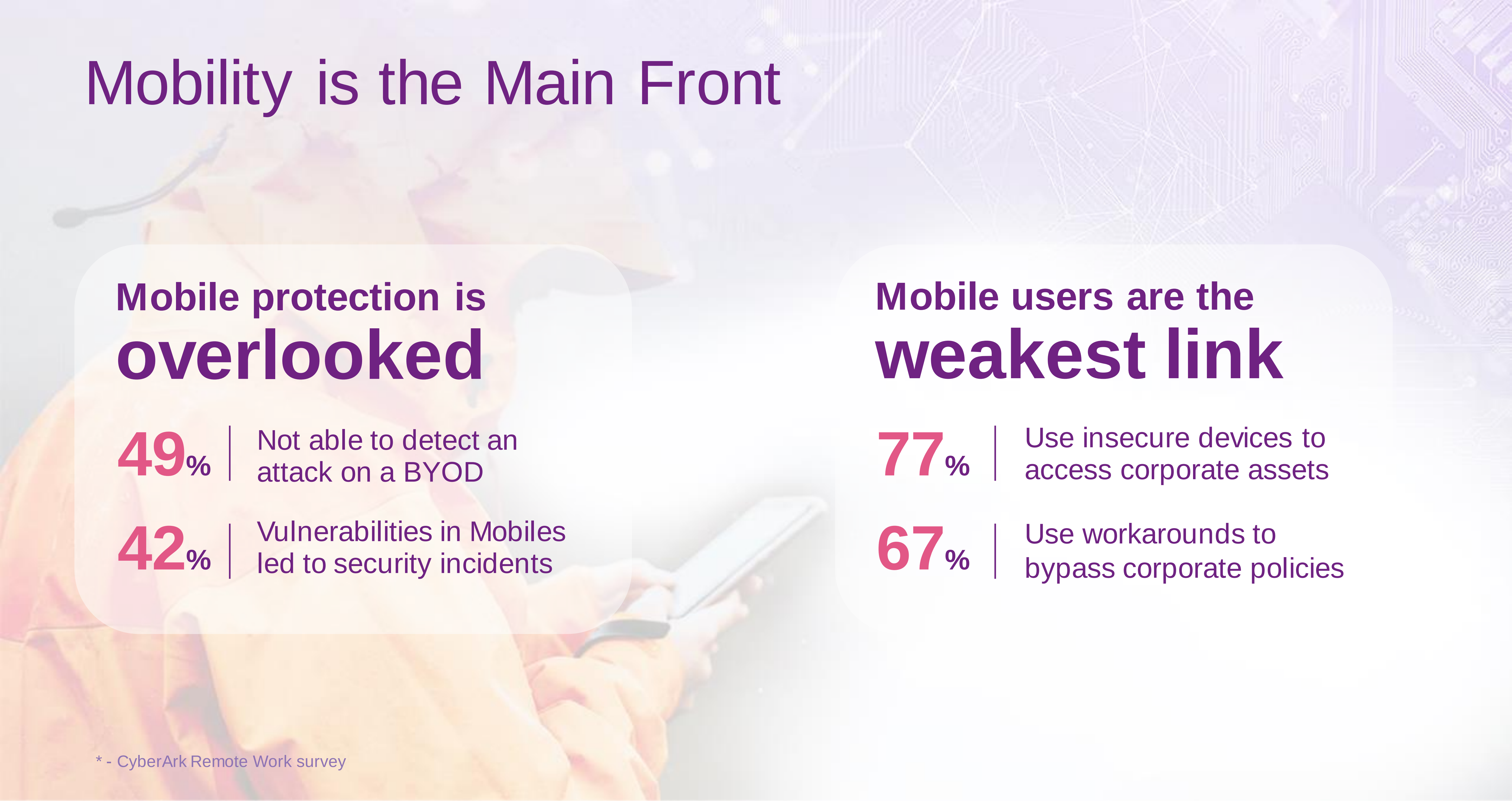
Harmony
Mobile

PROTECT YOUR MOBILE WORKFORCE

CHECK POINT™

Mobility is the Main Front



Mobile protection is **overlooked**

49% | Not able to detect an attack on a BYOD

42% | Vulnerabilities in Mobiles led to security incidents

Mobile users are the **weakest link**

77% | Use insecure devices to access corporate assets

67% | Use workarounds to bypass corporate policies

* - CyberArk Remote Work survey

MDM/UEM is **NOT** Security

	MDM / UEM	MTD
Malicious apps	✗	✓
Phishing	✗	✓
Zero-day phishing	✗	✓
Malicious files	✗	✓
Secure browsing	✗	✓
Bots	✗	✓
Man in the middle	✗	✓
OS vulnerabilities	●	✓
Device level exploits	✗	✓
Risky configuration	✓	✓
Rooting/jailbreak	●	✓
Storage scanning	✗	✓
Protected DNS	✗	✓

Main UEM in the Market

Microsoft Intune

mobileiron

vmware Workspace ONE

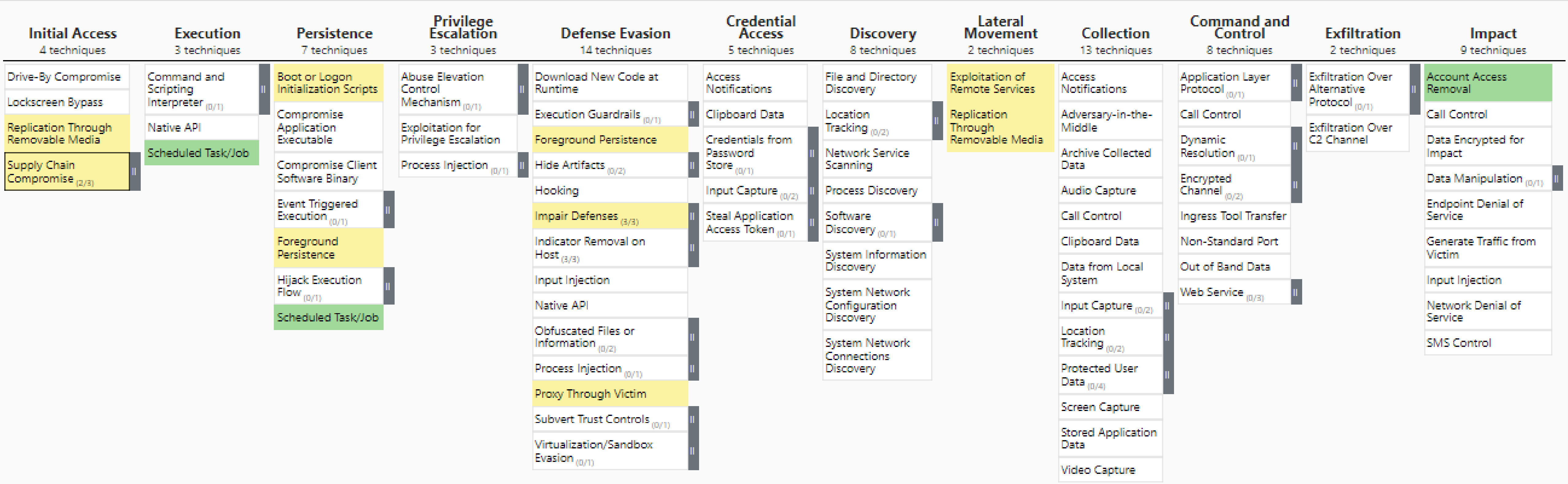
SAMSUNG Knox

CiTRIX XenMobile

jamf

MITRE ATT&CK Coverage

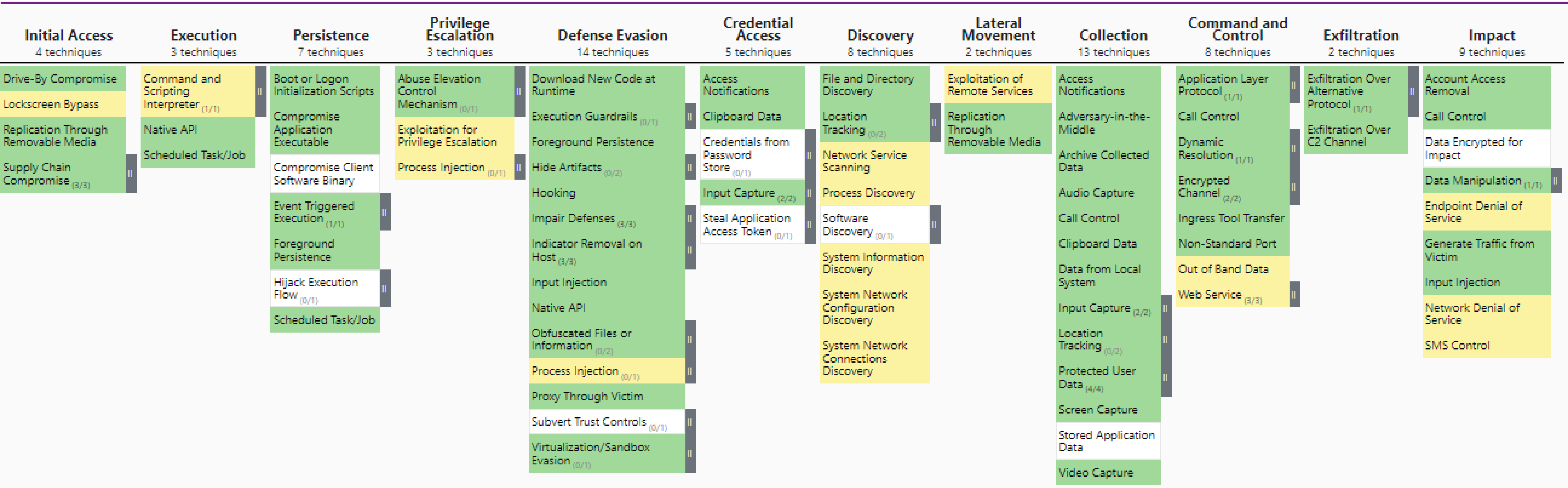
with UEM only



Initial Access 4 techniques	Execution 3 techniques	Persistence 7 techniques	Privilege Escalation 3 techniques	Defense Evasion 14 techniques	Credential Access 5 techniques	Discovery 8 techniques	Lateral Movement 2 techniques	Collection 13 techniques	Command and Control 8 techniques	Exfiltration 2 techniques	Impact 9 techniques
Drive-By Compromise	Command and Scripting Interpreter (0/1)	🟨 Boot or Logon Initialization Scripts	Abuse Elevation Control Mechanism (0/1)	Download New Code at Runtime	Access Notifications	File and Directory Discovery	🟨 Exploitation of Remote Services	Access Notifications	Application Layer Protocol (0/1)	Exfiltration Over Alternative Protocol (0/1)	🟩 Account Access Removal
Lockscreen Bypass	Native API	Compromise Application Executable	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Clipboard Data	Location Tracking (0/2)	🟨 Replication Through Removable Media	Adversary-in-the-Middle	Call Control	Exfiltration Over C2 Channel	Call Control
🟨 Replication Through Removable Media	🟩 Scheduled Task/Job	Compromise Client Software Binary	Process Injection (0/1)	🟨 Foreground Persistence	Credentials from Password Store (0/1)	Network Service Scanning		Archive Collected Data	Dynamic Resolution (0/1)		Data Encrypted for Impact
🟨 Supply Chain Compromise (2/3)		Event Triggered Execution (0/1)		Hide Artifacts (0/2)	Input Capture (0/2)	Process Discovery		Audio Capture	Encrypted Channel (0/2)		Data Manipulation (0/1)
		🟨 Foreground Persistence		Hooking	Steal Application Access Token (0/1)	Software Discovery (0/1)		Call Control	Ingress Tool Transfer		Endpoint Denial of Service
		Hijack Execution Flow (0/1)		🟨 Impair Defenses (3/3)		System Information Discovery		Clipboard Data	Non-Standard Port		Generate Traffic from Victim
		🟩 Scheduled Task/Job		Indicator Removal on Host (3/3)		System Network Configuration Discovery		Data from Local System	Out of Band Data		Input Injection
				Input Injection		System Network Connections Discovery		Input Capture (0/2)	Web Service (0/3)		Network Denial of Service
				Native API				Location Tracking (0/2)			SMS Control
				Obfuscated Files or Information (0/2)				Protected User Data (0/4)			
				Process Injection (0/1)				Screen Capture			
				🟨 Proxy Through Victim				Stored Application Data			
				Subvert Trust Controls (0/1)				Video Capture			
				Virtualization/Sandbox Evasion (0/1)							

MITRE ATT&CK Coverage

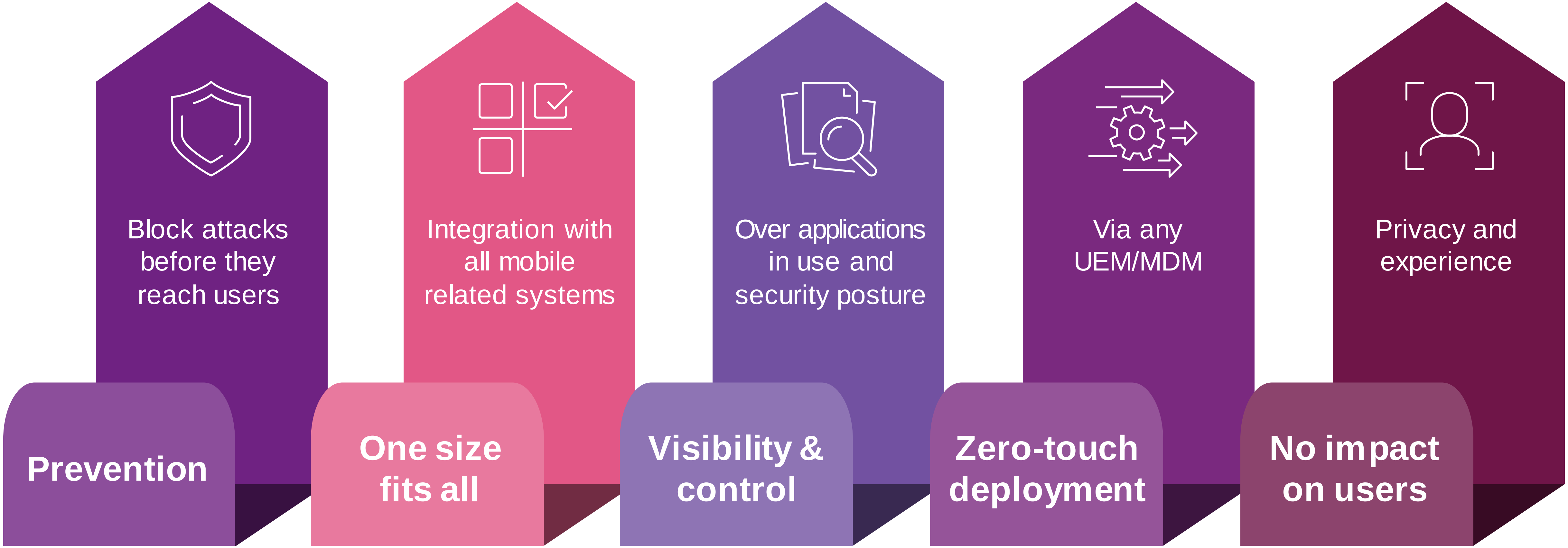
with Harmony Mobile & UEM



Initial Access 4 techniques	Execution 3 techniques	Persistence 7 techniques	Privilege Escalation 3 techniques	Defense Evasion 14 techniques	Credential Access 5 techniques	Discovery 8 techniques	Lateral Movement 2 techniques	Collection 13 techniques	Command and Control 8 techniques	Exfiltration 2 techniques	Impact 9 techniques
🟩 Drive-By Compromise	🟨 Command and Scripting Interpreter (1/1)	🟩 Boot or Logon Initialization Scripts	🟩 Abuse Elevation Control Mechanism (0/1)	🟩 Download New Code at Runtime	🟩 Access Notifications	🟩 File and Directory Discovery	🟨 Exploitation of Remote Services	🟩 Access Notifications	🟩 Application Layer Protocol (1/1)	🟩 Exfiltration Over Alternative Protocol (1/1)	🟩 Account Access Removal
🟨 Lockscreen Bypass	🟩 Native API	🟩 Compromise Application Executable	🟨 Exploitation for Privilege Escalation	🟩 Execution Guardrails (0/1)	🟩 Clipboard Data	🟩 Location Tracking (0/2)	🟩 Replication Through Removable Media	🟩 Adversary-in-the-Middle	🟩 Call Control	🟩 Exfiltration Over C2 Channel	🟩 Call Control
🟩 Replication Through Removable Media	🟩 Scheduled Task/Job	⬜ Compromise Client Software Binary	🟨 Process Injection (0/1)	🟩 Foreground Persistence	⬜ Credentials from Password Store (0/1)	🟨 Network Service Scanning		🟩 Archive Collected Data	🟩 Dynamic Resolution (1/1)		⬜ Data Encrypted for Impact
🟩 Supply Chain Compromise (3/3)		🟩 Event Triggered Execution (1/1)		🟩 Hide Artifacts (0/2)	🟩 Input Capture (2/2)	🟨 Process Discovery		🟩 Audio Capture	🟩 Encrypted Channel (2/2)		🟩 Data Manipulation (1/1)
		🟩 Foreground Persistence		🟩 Hooking	⬜ Steal Application Access Token (0/1)	⬜ Software Discovery (0/1)		🟩 Call Control	🟩 Ingress Tool Transfer		🟨 Endpoint Denial of Service
		⬜ Hijack Execution Flow (0/1)		🟩 Impair Defenses (3/3)		🟨 System Information Discovery		🟩 Clipboard Data	🟩 Non-Standard Port		🟩 Generate Traffic from Victim
		🟩 Scheduled Task/Job		🟩 Indicator Removal on Host (3/3)		🟨 System Network Configuration Discovery		🟩 Data from Local System	🟨 Out of Band Data		🟩 Input Injection
				🟩 Input Injection		🟨 System Network Connections Discovery		🟩 Input Capture (2/2)	🟨 Web Service (3/3)		🟨 Network Denial of Service
				🟩 Native API				🟩 Location Tracking (0/2)			🟨 SMS Control
				🟩 Obfuscated Files or Information (0/2)				🟩 Protected User Data (4/4)			
				🟨 Process Injection (0/1)				🟩 Screen Capture			
				🟩 Proxy Through Victim				⬜ Stored Application Data			
				⬜ Subvert Trust Controls (0/1)				🟩 Video Capture			
				🟩 Virtualization/Sandbox Evasion (0/1)							

5 Key Principles for Choosing

The Optimal Mobile Security Solution



Block attacks before they reach users

Prevention

Integration with all mobile related systems

One size fits all

Over applications in use and security posture

Visibility & control

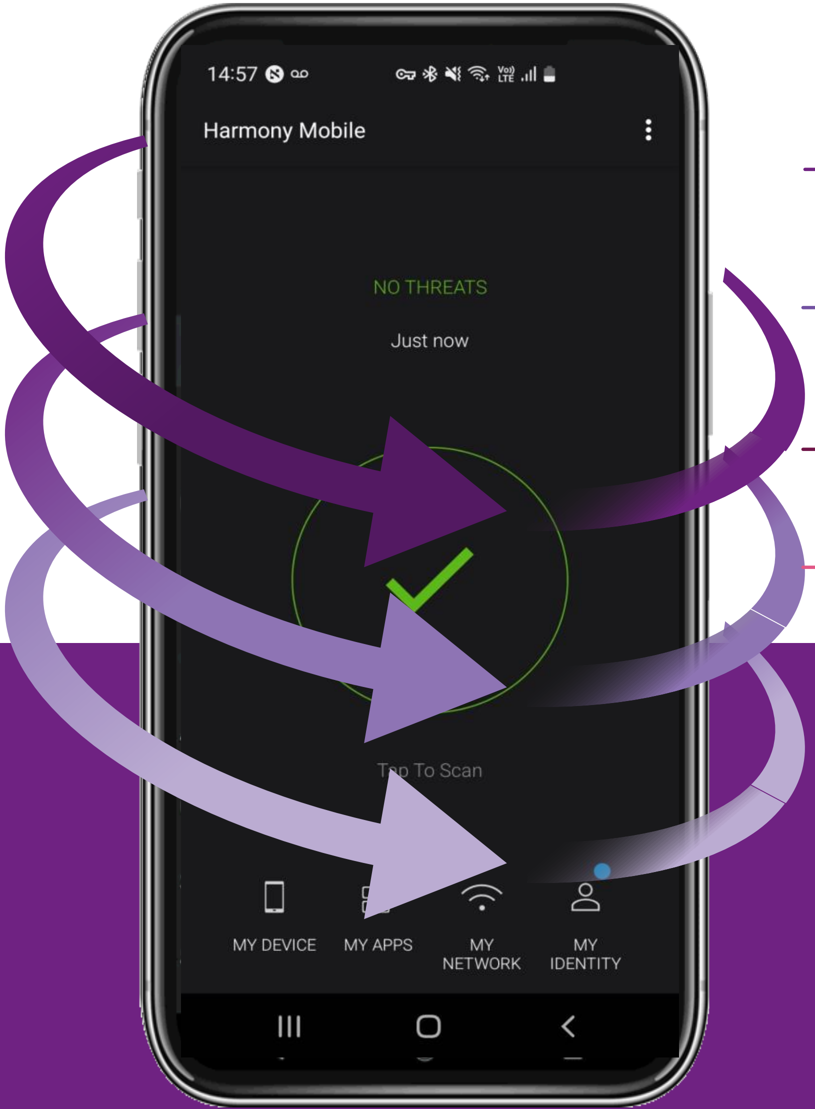
Via any UEM/MDM

Zero-touch deployment

Privacy and experience

No impact on users

Harmony Mobile 4.1 - Complete Protection



01 APPLICATIONS

02 NETWORK

03 DEVICE & OS

04 FILES

01

BEHAVIORAL RISK ENGINE

Real-time analysis

Malicious side-loading prevention

02

- Anti-phishing / Zero-phishing
- Safe browsing
- Conditional access
- Anti-bot
- URL filtering
- Protected DNS
- Wi-Fi network security (MiTM)
- Risky download prevention

03

Device risk assessment:

- OS vulnerabilities
- Device-level exploits
- Risky configurations
- Advanced rooting
- Jailbreak detection

04

Files

- Download prevention
- Storage scanning (Android)
- File Emulation

File Protection

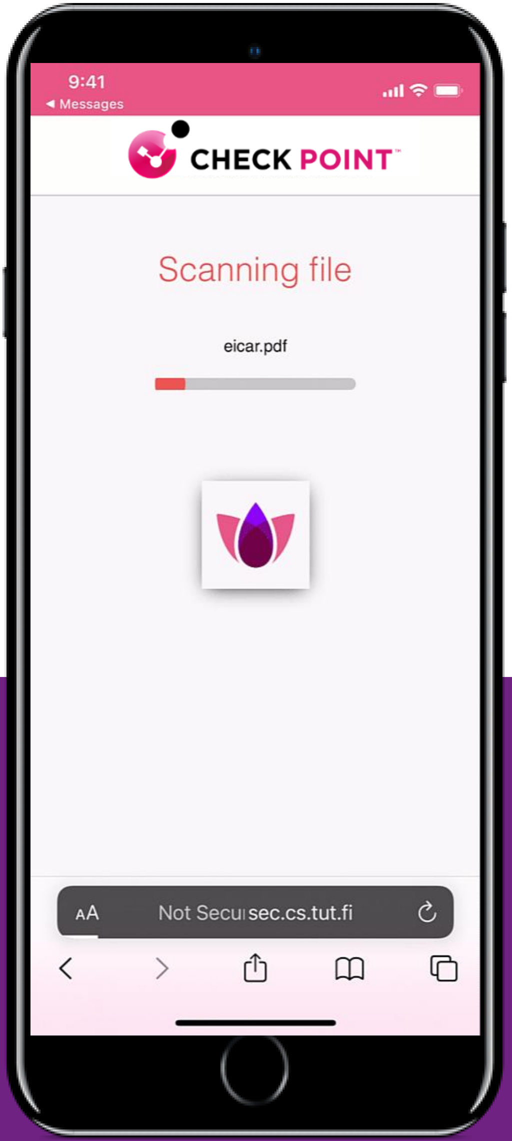
Any file downloaded is scanned

All file types are supported

Unknown files are uploaded to a sandbox

Using ThreatCloud intelligence

If risky, download is blocked and threat details are visible



NEW

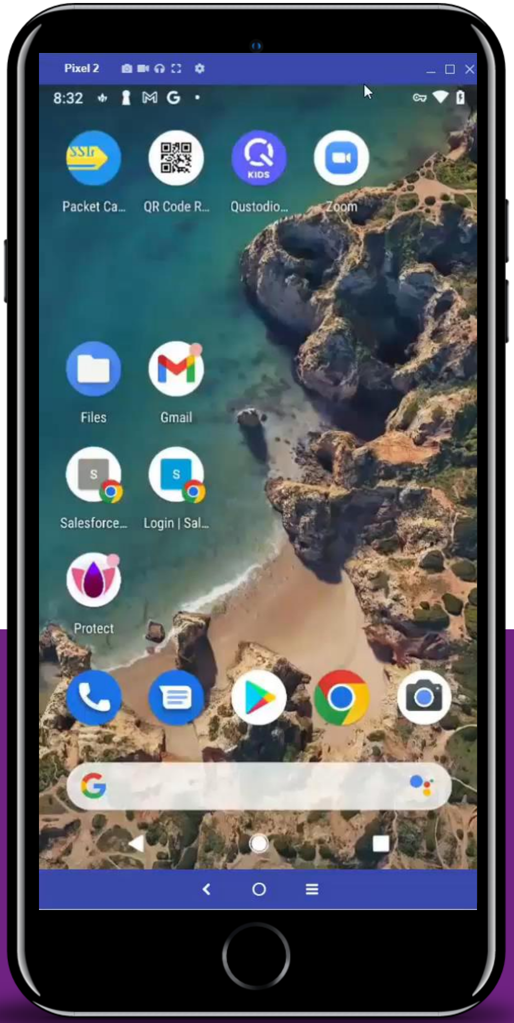
File sandboxing available now.
Enable it to catch zero-day attacks!

Phishing and Zero-day Phishing Protection

Prevent Identity Theft

1 User receives a message with a link

2 URL identified as malicious phishing and blocked

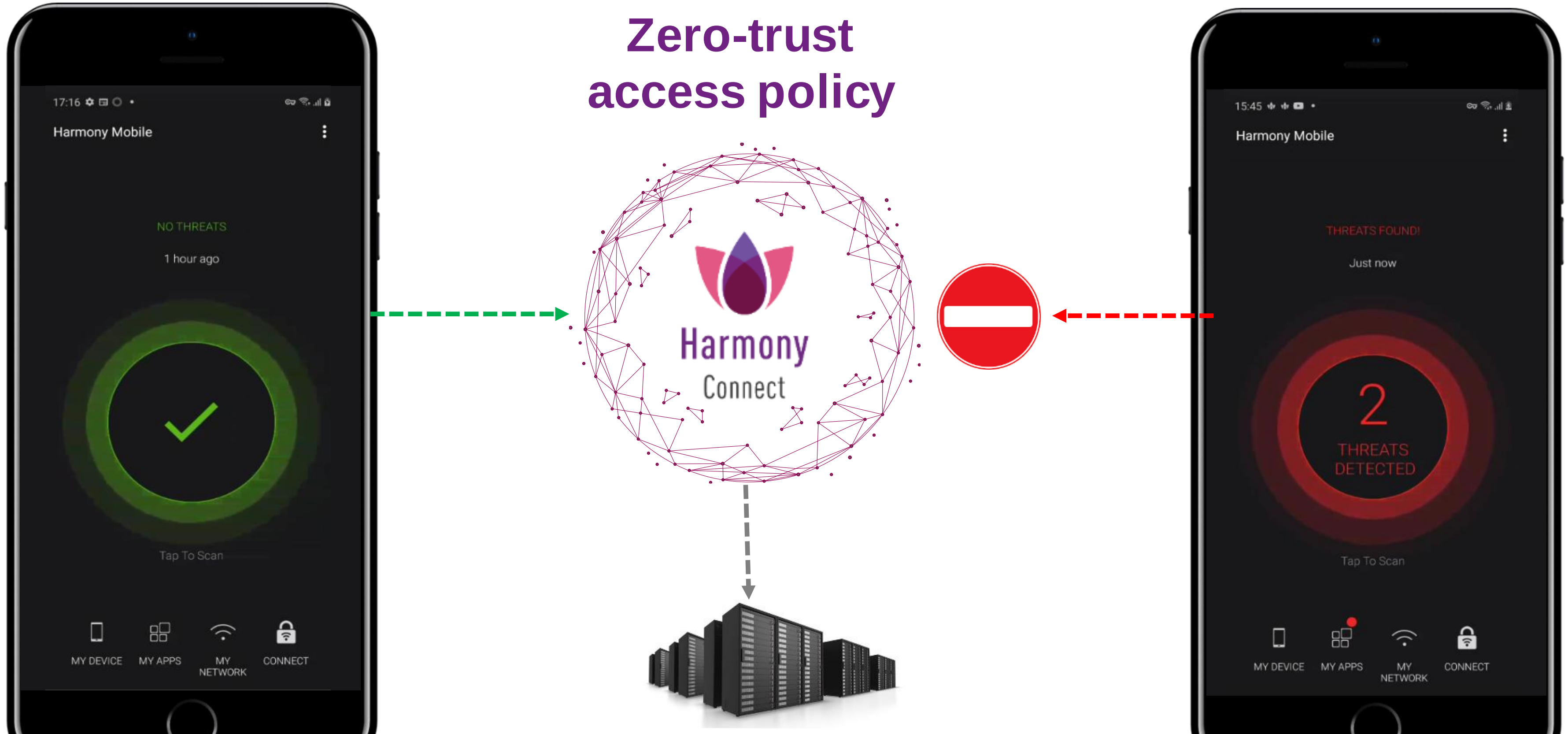


3 Anti-phishing engine instantly inspects the link

Unknown sites analyzed in real-time with Zero-phishing

SMS Phishing Preventive Quarantine available now!

Secured Remote Access with Harmony Connect



Zero-trust access policy

Corporate applications

Full Flexibility

All Leading MDM/UEMs, BYOD or COPE

MDM/UEM

- Microsoft Intune 1 CLICK
- BlackBerry UEM
- vmware Workspace ONE 1 CLICK
- SAMSUNG Knox
- mobileiron
- jamf
- IBM MaaS360
- G
- CITRIX XenMobile

LOG INTELLIGENCE

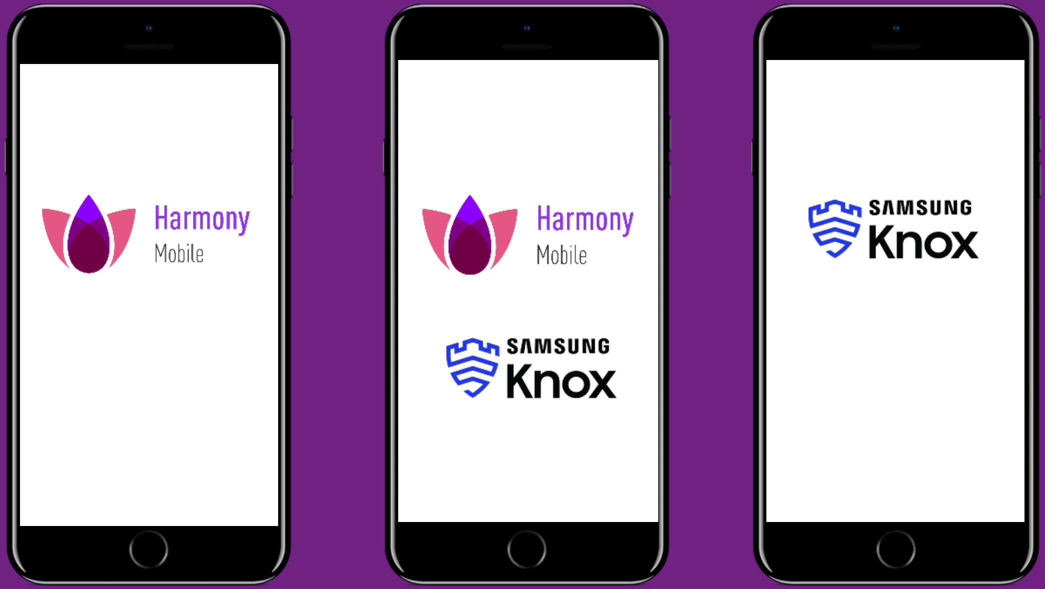
- splunk>
- rsyslog
- vmware VMware Workspace ONE Intelligence
- Microsoft Defender Advanced Threat Protection
- ArcSight
- HORIZON Unified Management and Security Operations

Samsung Knox Integration

Harmony Mobile – The only leading solution to integrate with both Knox MDM & Knox Agent

Prevent malicious apps from running

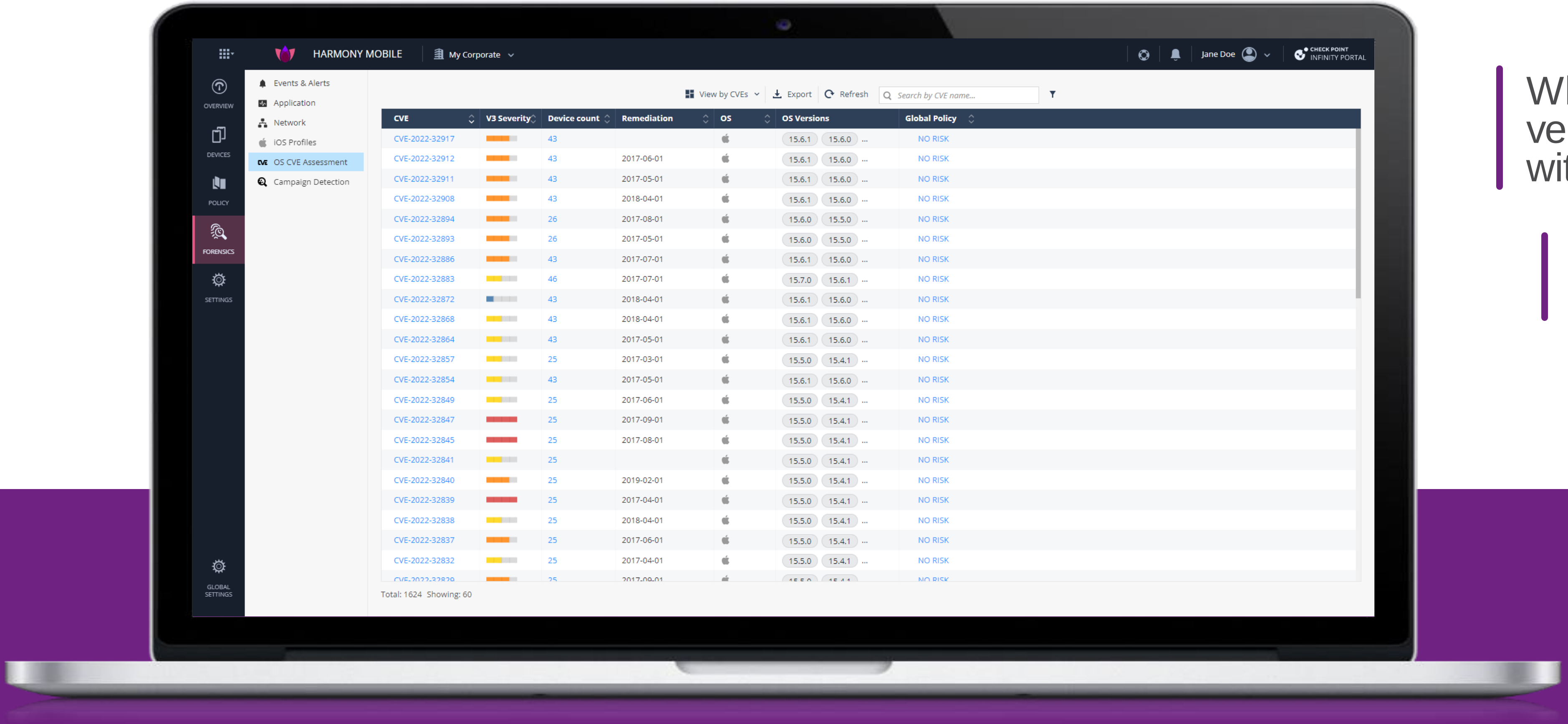
Prevent malicious application installation



Prevent malware from interfering with the Harmony Mobile app activity

Certification and Compliance

OS and App CVE Assessment



CVE	V3 Severity	Device count	Remediation	OS	OS Versions	Global Policy
CVE-2022-32917	🟧	43			15.6.1 15.6.0 ...	NO RISK
CVE-2022-32912	🟧	43	2017-06-01		15.6.1 15.6.0 ...	NO RISK
CVE-2022-32911	🟧	43	2017-05-01		15.6.1 15.6.0 ...	NO RISK
CVE-2022-32908	🟧	43	2018-04-01		15.6.1 15.6.0 ...	NO RISK
CVE-2022-32894	🟧	26	2017-08-01		15.6.0 15.5.0 ...	NO RISK
CVE-2022-32893	🟧	26	2017-05-01		15.6.0 15.5.0 ...	NO RISK
CVE-2022-32886	🟧	43	2017-07-01		15.6.1 15.6.0 ...	NO RISK
CVE-2022-32883	🟨	46	2017-07-01		15.7.0 15.6.1 ...	NO RISK
CVE-2022-32872	🟦	43	2018-04-01		15.6.1 15.6.0 ...	NO RISK
CVE-2022-32868	🟨	43	2018-04-01		15.6.1 15.6.0 ...	NO RISK
CVE-2022-32864	🟨	43	2017-05-01		15.6.1 15.6.0 ...	NO RISK
CVE-2022-32857	🟨	25	2017-03-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32854	🟨	43	2017-05-01		15.6.1 15.6.0 ...	NO RISK
CVE-2022-32849	🟨	25	2017-06-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32847	🟥	25	2017-09-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32845	🟥	25	2017-08-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32841	🟨	25			15.5.0 15.4.1 ...	NO RISK
CVE-2022-32840	🟧	25	2019-02-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32839	🟥	25	2017-04-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32838	🟨	25	2018-04-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32837	🟧	25	2017-06-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32832	🟨	25	2017-04-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32829	🟧	25	2017-09-01		15.5.0 15.4.1 ...	NO RISK

Total: 1624 Showing: 60

Which OS versions running with CVEs

Set a policy or risk per CVE

CHECK POINT

Elegant User Experience

VIRTUALLY ZERO IMPACT ON:

Privacy by design

Browsing experience

Battery life

Data/CPU consumption

Harmony Mobile

COMPLETE PROTECTION

Protecting corporate data across the mobile attack surface: apps, networks, OS and files

SIMPLE MANAGEMENT

From no protection to tens of thousands of protected devices within minutes

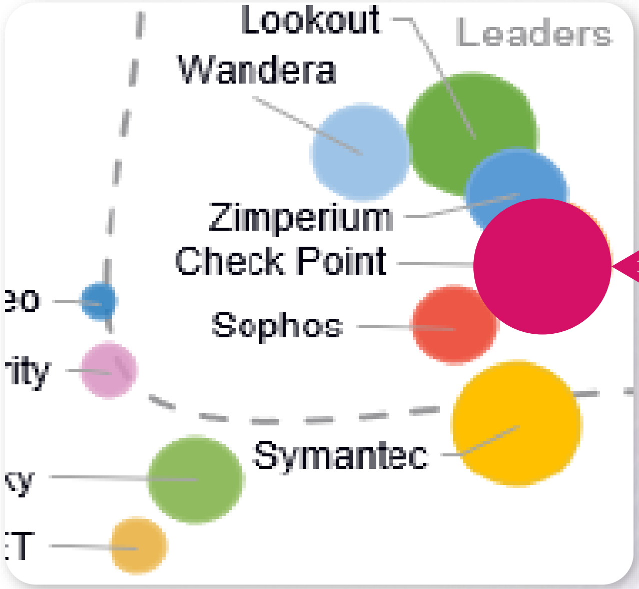
USER FRIENDLY

Zero impact on user experience or privacy

Leading the MTD Market

Gartner · IDC Analyze the Future · OMDIA · FROST & SULLIVAN · Miercom · analysys mason

“Harmony Mobile **detected 100%** of browsing, privacy invasions, network-based and device-based threats and vulnerabilities. Its combination of refined remediation tools and easily navigated interface **made stopping threats effortless**.”



Check Point

CHECK POINT™

YOU DESERVE THE BEST SECURITY

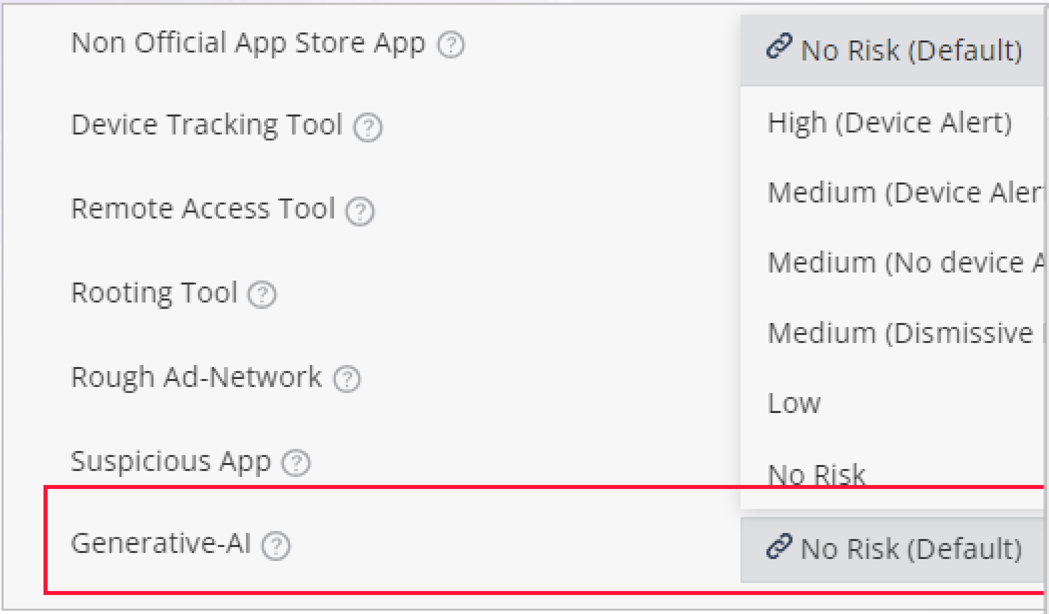
HARMONY MOBILE

WHAT’S NEXT FOR 2023

Protection against AI-driven threats

COMING SOON

- Protection against Generative AI apps
- Ne
- DL



Non Official App Store App ? — No Risk (Default)

Device Tracking Tool ?

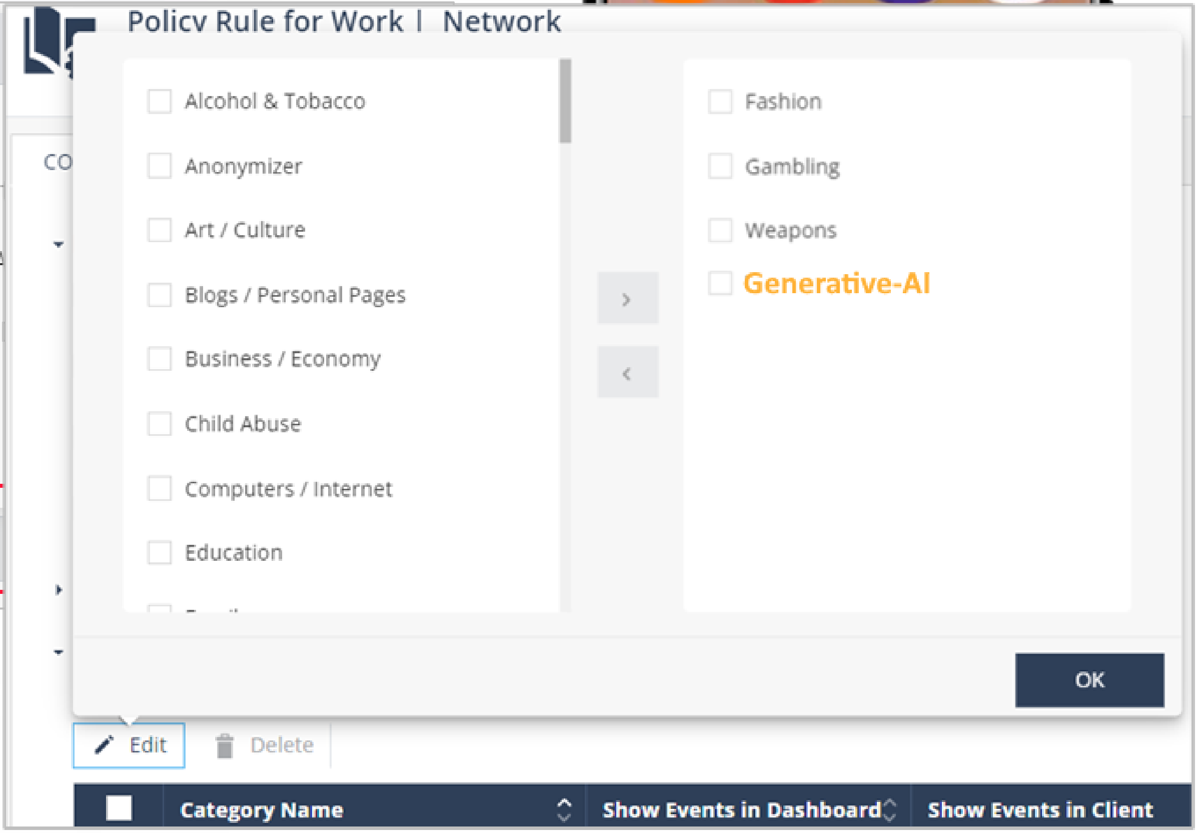
Remote Access Tool ?

Rooting Tool ?

Rough Ad-Network ?

Suspicious App ?

Generative-AI ? — No Risk (Default)



Policy Rule for Work | Network

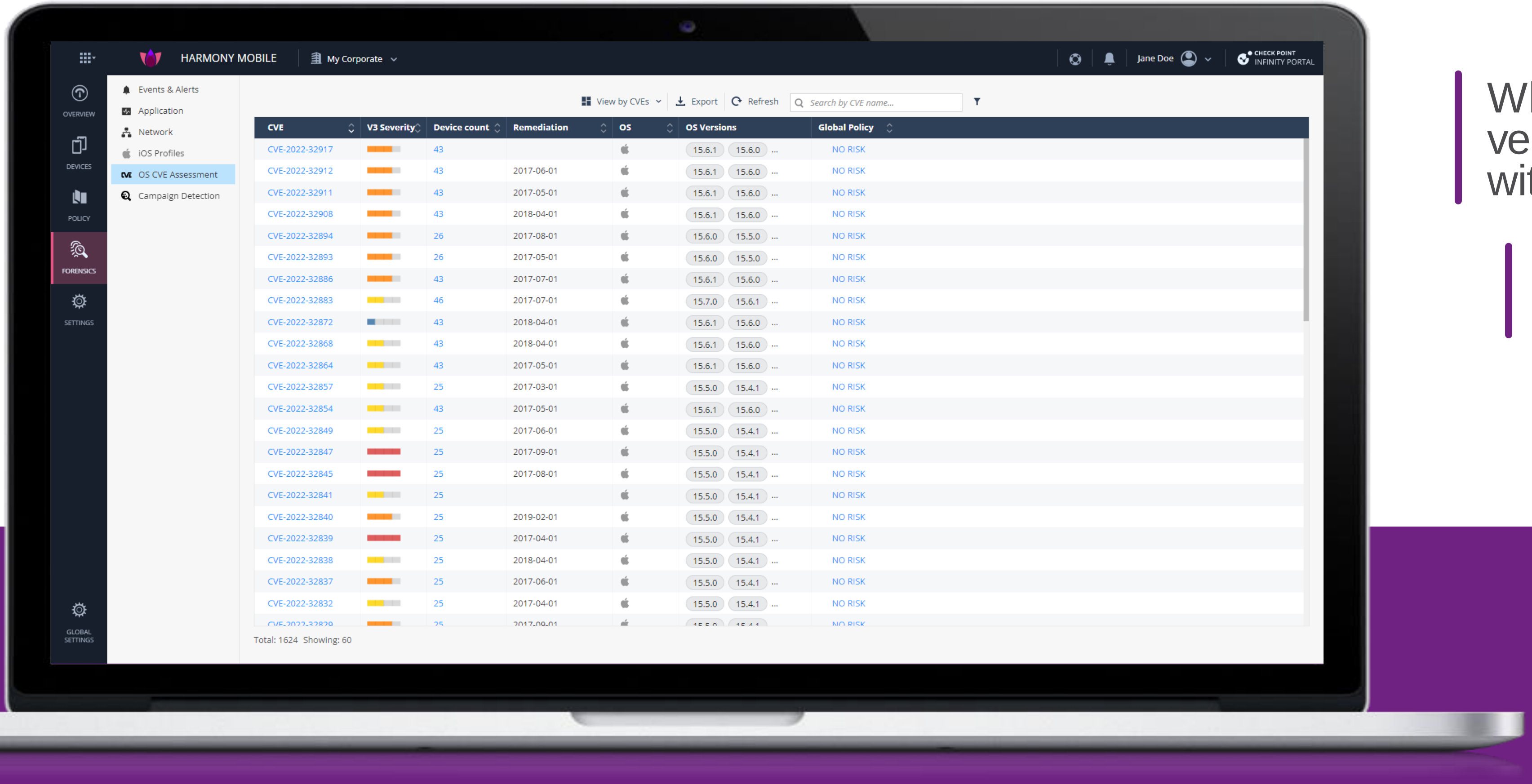
□ Alcohol & Tobacco
□ Anonymizer
□ Art / Culture
□ Blogs / Personal Pages
□ Business / Economy
□ Child Abuse
□ Computers / Internet
□ Education

□ Fashion
□ Gambling
□ Weapons
□ Generative-AI

□	Category Name	Show Events in Dashboard	Show Events in Client

Certification and Compliance

OS and App CVE Assessment



CVE	V3 Severity	Device count	Remediation	OS	OS Versions	Global Policy
CVE-2022-32917	🟧	43			15.6.1 15.6.0 ...	NO RISK
CVE-2022-32912	🟧	43	2017-06-01		15.6.1 15.6.0 ...	NO RISK
CVE-2022-32911	🟧	43	2017-05-01		15.6.1 15.6.0 ...	NO RISK
CVE-2022-32908	🟧	43	2018-04-01		15.6.1 15.6.0 ...	NO RISK
CVE-2022-32894	🟧	26	2017-08-01		15.6.0 15.5.0 ...	NO RISK
CVE-2022-32893	🟧	26	2017-05-01		15.6.0 15.5.0 ...	NO RISK
CVE-2022-32886	🟧	43	2017-07-01		15.6.1 15.6.0 ...	NO RISK
CVE-2022-32883	🟨	46	2017-07-01		15.7.0 15.6.1 ...	NO RISK
CVE-2022-32872	🟦	43	2018-04-01		15.6.1 15.6.0 ...	NO RISK
CVE-2022-32868	🟨	43	2018-04-01		15.6.1 15.6.0 ...	NO RISK
CVE-2022-32864	🟨	43	2017-05-01		15.6.1 15.6.0 ...	NO RISK
CVE-2022-32857	🟨	25	2017-03-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32854	🟨	43	2017-05-01		15.6.1 15.6.0 ...	NO RISK
CVE-2022-32849	🟨	25	2017-06-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32847	🟥	25	2017-09-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32845	🟥	25	2017-08-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32841	🟨	25			15.5.0 15.4.1 ...	NO RISK
CVE-2022-32840	🟧	25	2019-02-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32839	🟥	25	2017-04-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32838	🟨	25	2018-04-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32837	🟧	25	2017-06-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32832	🟨	25	2017-04-01		15.5.0 15.4.1 ...	NO RISK
CVE-2022-32829	🟧	25	2017-09-01		15.5.0 15.4.1 ...	NO RISK

Total: 1624 Showing: 60

Which OS versions running with CVEs

App CVE Visibility COMING SOON

Set a policy or risk per CVE

Mobile Security offering by Check Point

Harmony Mobile

Managed Security Solution
for businesses

ZoneAlarm

Consumer – unmanaged solution

Harmony App Protect

Protecting Your own Apps

SDK ➡

Yearly Subscription
User / Device based license

Consumption PAYG
via MSP / MSSP

Summary

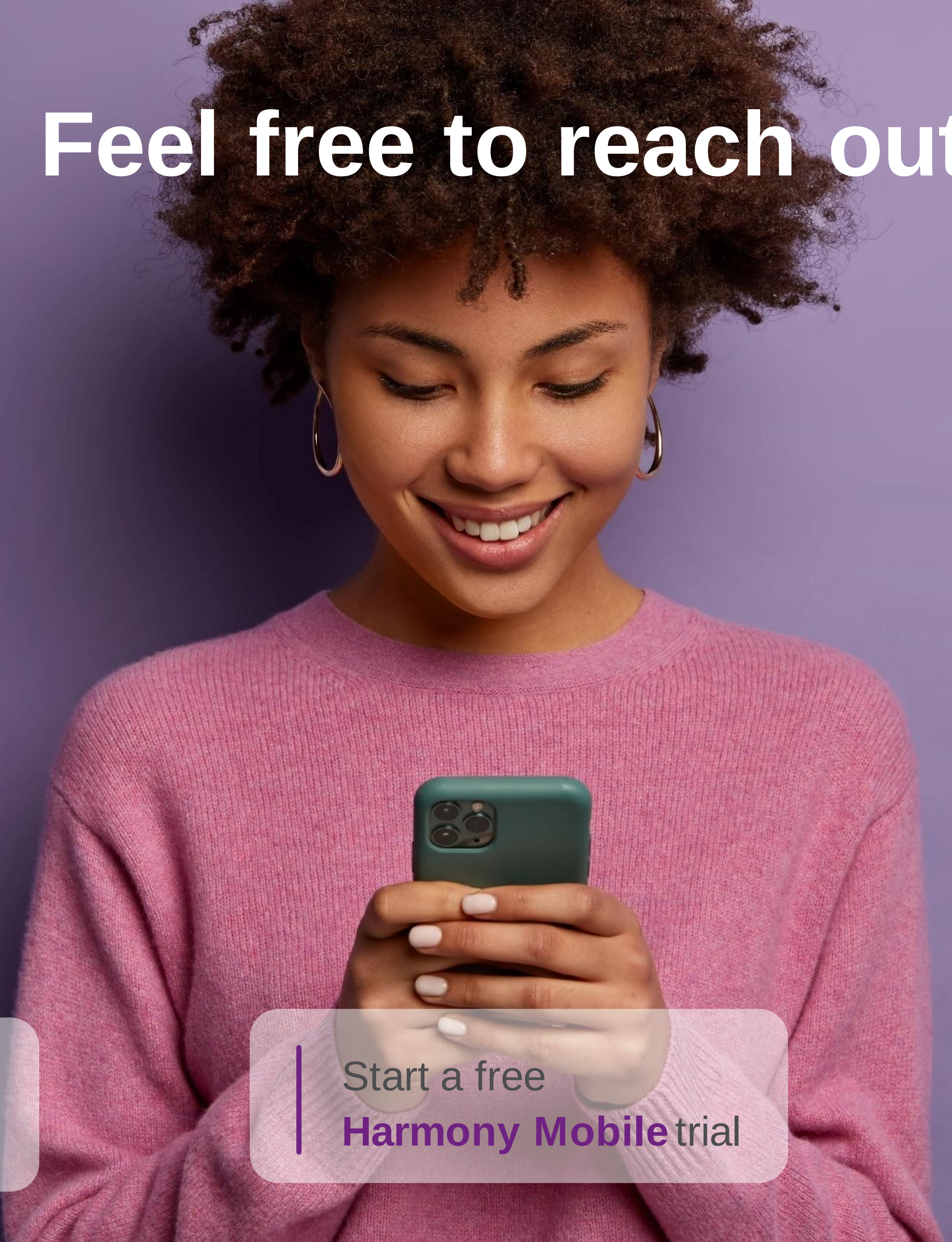
- EVER EVOLVING MOBILE SECURITY THREAT LANDSCAPE

- MOBILE IS THE WEAKEST SECURITY LINK
  Mobile attacks are on the rise
  MDM is not enough

- YOU NEED AN MTD TO PROTECT YOUR ORGANIZATION

- HARMONY MOBILE IS THE
  BEST SOLUTION FOR YOU
  Best security
  Easy to deploy and manage
  Market leader according to analysts

Feel free to reach out!



Harmony Mobile

Register for a **DEMO** with a Security Expert

Start a free **Harmony Mobile** trial

Watch the **product tour video**

CHECK POINT™

Harmony
Mobile

THANK YOU