KNOVATION
SOLUTIONS

Secure Mobile

The AI Attack Surface: Your Employees' Mobile Devices Are Becoming the New Security Perimeter

Protect the person. Protect the device. Protect the business.

KNOVATION SOLUTIONS

Introduction

AI has changed the economics of cyberattacks. Secure Mobile protects the last mile, the mobile device where your people receive, trust and act on those attacks. Traditional security protects the infrastructure. But increasingly, the attack starts with a person, often through a mobile device.

The new threat: AI is changing cybercrime in three important ways:

1. More convincing attacks

Generative AI enables attackers to create highly personalised phishing, smishing and social-engineering attacks with better language, context and targeting.

2. More attacks, at greater scale

Attackers can automate reconnaissance, content creation and campaign execution, allowing them to target thousands of employees rather than a handful.

3. Faster adaptation

AI allows attackers to rapidly modify campaigns when organisations introduce new controls, making static security controls increasingly difficult to rely on.

The result: The human is becoming an increasingly attractive attack surface, and the mobile phone is one of the most effective ways to reach them.

Business Challenges

AI has weaponised Mobile Phishing

AI is making phishing and social engineering: faster, more convincing, more personalised and easier to scale.

Attackers have adopted AI faster than most enterprises have adopted mobile security.

Generative AI now writes the lures and clones the voices, turning mobile phishing, smishing, and device compromise into a scalable, highly convincing attack channel. No single tool closes this gap alone: it takes management, detection, and containment working together across the entire device fleet

380% growth in phishing events detected on employee mobile devices since Jan 2025	**86%** of phishing attacks now contain AI-generated content	**40% higher** success rate for mobile phishing than email-based attacks	**1 in 10** mobile devices now carry spyware, a 4x jump year-on-year

"AI has changed the game on securing mobile. It's making mobile attacks easier, scalable, and much more sophisticated." - Shridhar Mittal, CEO, Zimperium

Why One Layer Is Not Enough

AI hasn't just made attacks more convincing, it's made them faster to generate, cheaper to run, and able to hit every layer of the stack at once. A single tool built for a single job can't keep up with an attacker who can retool in minutes.

- **Management is not detection**. UEM/MDM configures devices, enforces policy, and automates patching, but policy is static and AI-generated attacks are not. It isn't built to detect an active AI-crafted phishing attempt, a malicious app, or a hostile network the moment it happens.
- **Detection is not containment**. AI-generated malware is built to move and mutate fast. Spotting one instance on one device doesn't stop the next variant from reaching the next endpoint, and without automated containment, a single AI-driven compromise can become a fleet-wide incident before a human ever sees an alert.
- **Mobile-only coverage leaves the rest of the fleet exposed**. AI-driven campaigns don't stop at mobile; the same phishing kits and malware families increasingly target laptops and desktops too. Mobile threat detection protects phones and tablets, but the rest of the fleet needs its own zero-trust prevention layer, or it becomes the softer target.
- **Point tools create blind spots between the gaps.** AI-driven attacks are specifically built to probe for the seams between tools: the device type, channel, or vendor boundary nothing is watching. A resilient stack needs management, detection, and response to share context, not operate in silos.

KNOVATION SOLUTIONS

Key capabilities

Beating an AI-speed attacker takes a stack that doesn't depend on recognising an attack it has seen before. Each layer below plays a distinct, complementary role.

Layer 1: Manage, with Ivanti UEM & MDM

UEM manages and secures the full device fleet, mobile, desktop and everything in between, from one console, with AI-driven automation that closes the door on vulnerabilities before AI-powered attackers can find and weaponise them.

Cross-platform management	Manages iOS, Android, Windows, macOS, ChromeOS, Linux, and rugged devices from a single console.
Autonomous self-healing	AI-driven automation resolves common device issues silently in the background, without a help desk ticket.
Patch automation	AI-prioritised, automated patching closes vulnerabilities at the same machine speed AI-driven scanning tools use to find and exploit them.
Lifecycle management	Handles onboarding, provisioning, policy enforcement, and secure retirement across the device lifecycle.

Layer 2: Detect, with Ivanti Mobile Threat Defence powered by Zimperium

MTD is an on-device, machine-learning-powered defence that fills the gap the management layer can't cover real-time detection of device, network, phishing, and app-based attacks, including AI-generated and AI-obfuscated threats that have no known signature to match against, working even offline.

Device threats	Behavioural, ML-based detection catches OS exploits, jailbreak/root, and forensic tampering on-device, including novel, AI-crafted exploits with no prior signature.

Network threats	Identifies rogue Wi-Fi, man-in-the-middle attacks, and unsafe or spoofed networks, including AI-orchestrated network-level lures.
Phishing & Mishing	Stops AI-generated phishing, smishing, and messaging-app lures before employees click, the fastest-growing AI attack vector on mobile.
Native Ivanti integration	Feeds risk signals directly into Ivanti for automated, risk-based conditional access decisions the moment an AI-driven threat is detected.

Layer 3: Contain & Respond, with WatchGuard EPDR

EDR extends zero-trust protection to the rest of the fleet, the laptops and desktops working alongside managed mobile devices, combining prevention, detection, and automated containment in a single lightweight agent built to stop what signatures can't.

Zero trust by default	Denies unknown or untrusted applications automatically, instead of matching against known signatures, the exact defence AI-generated, self-mutating malware is designed to evade.
Lateral movement containment	Automatically isolates a compromised endpoint to stop an AI-accelerated attack from spreading across the network before a human can respond.
Full activity visibility	Maintains detailed endpoint activity logs for investigation, threat hunting, and compliance.
Low-noise, unified response	Combines prevention, detection, and response in one agent, keeping alert volume manageable even as AI-driven attack attempts scale up.

Layer 4: Knovation Services

Comprehensive mobile and endpoint visibility and management that eliminates security blind spots.

Assessments	• Mobile Risk Assessment • Endpoint Risk Assessment • Pentest • Attack Surface Monitoring
Pre-Sales Support	• Discovery & Requirements Definition • Scoping & Design • Solution Overview & Proposal Build • Demonstrations & POVs.
Managed Services	Technical Services • Policy definition, set up & onboarding, configuration, Integration, knowledge transfer Support Services • SLA, troubleshooting, optimisation, automated remediation, operational & governance health checks

Business Outcomes

Reducing the risk created by AI-enabled attacks reaching your workforce through mobile devices.

- Reduce the likelihood of successful mobile compromise by protecting users beyond traditional email security
- Extend security controls to employee-owned devices and protect devices accessing business information
- Increase security visibility and identify mobile threats earlier
- Strengthen mobile security governance by extending Zero Trust to mobile
- Reduce the likelihood of mobile compromise becoming a wider incident

From Exposure to Governed Control

AI has not created a new category of attack. It has made the existing one cheap enough to run at scale, and convincing enough to succeed on the device your people trust most. Management alone cannot detect it, detection alone cannot contain it, and a mobile-only view leaves the rest of the fleet as the softer target.

Secure Mobile closes that gap by running management, detection and containment as one architecture rather than three tools with three separate blind spots. Knovation Solutions delivers, integrates and supports the full stack as a single point of accountability.

Start with a Secure Mobile Risk Assessment to establish where the exposure sits across your existing devices, then scale the architecture to the risk it uncovers.

Next Steps

Contact Knovation Solutions for a Secure Mobile Risk Assessment

AI can create the attack. Knovation Solutions helps stop it at the device.

Knovation Solutions:

Website: www.knovation.co.za

Call: +27 83 326 1198

Email: info@knovation.co.za

Where Control Becomes Confidence

KNOVATION
SOLUTIONS