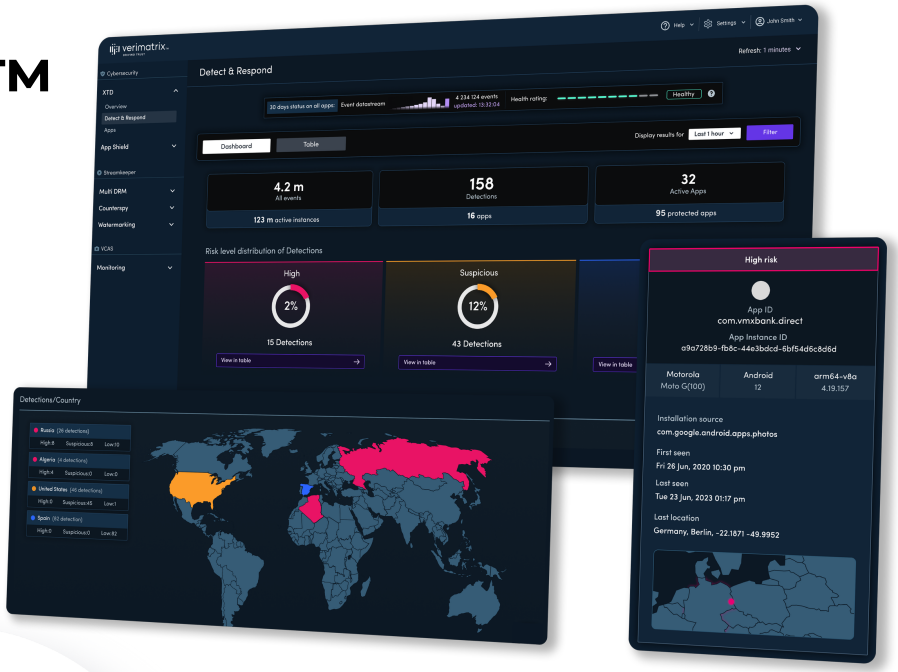
verimatrix cybersecurity

#1 Mobile App Security

Verimatrix XTD™

- Shield your Android and iOS apps in minutes.
- Prevent malware, reverse engineering & more.
- Help developers meet compliance obligations.



Empower & Detect with XTD

Man-in-the-Middle attacks, Reverse Engineering, Geo-compliance, Rootkit, Tampering, Hooking, Debugger, Emulator, Overlay, Repackaging, Bootloader Unlocked, Frida, Memory Editing/Injection, Unauthorized DNS, VPN/Proxy detection, Android accessibility API abuse, and more!

Depth of Verimatrix XTD App Security
XTD Mobile Android & iOS
XTD Embedded / Desktop
XTD Web Applications
XTD Native for iOS & Android
XTD Enterprise Detection & Response
XTD Whitebox Cryptography
XTD Premium Support
XTD Managed Services

Key Verimatrix Advantages

- Pro DevSecOps tools like code obfuscation
- Enterprise platform: Detect & respond in real-time to threats
- AI/ML malware detection
- Seamless CI/CD integration
- Addresses OWASP Mobile Top 10 vulnerabilities

Verimatrix's Flexible Deployment

- On-prem toolkits
- Zero code/cloud
- White glove "we do it for you" security

Verimatrix XTD Addresses all top 10 OWASP Mobile App Vulnerabilities

M1: Improper Credential Usage	Verimatrix Overlay Detector™ identifies and prevents unauthorized screen overlays that can capture sensitive user inputs like credentials, ensuring that they are only used in the intended, secure context of the app.
M2: Inadequate Supply Chain Security	Verimatrix Supply Chain Defender™ monitors app instances for backdoors, whitelists outgoing connections to detect and prevent unauthorized communications, and helps mitigate API risks in compromised mobile applications.
M3: Insecure Authentication / Authorization	Verimatrix Man-in-the-Middle Detection™ to detect attacks on certificate pinning.
M4: Insufficient Input / Output Validation	Verimatrix Anti-Tampering™ uses thousands of micro-checks within your app's code to prevent unauthorized mods and allows customizable security settings to address Insufficient I/O Validation by ensuring the app operates as designed.
M5: Insecure Communication	Verimatrix Man-in-the-Middle Interceptor™ detects and prevents man-in-the-middle attacks, where an attacker intercepts and potentially modifies communication between a mobile app and server.
M6: Inadequate Privacy Controls	Verimatrix Anti-debugging™, Verimatrix Anti-hooking™, Verimatrix Anti-tampering™ hardens the applications against attacks trying to extract private data.
M7: Insufficient Binary Protections	Verimatrix Anti-Debugger™, Verimatrix Anti-Hooking™, Verimatrix Anti-Tampering™.
M8: Security Misconfiguration	Verimatrix Anti-Debugger™ ensures applications are not debuggable once deployed, preventing alterations to the app's runtime environment, which helps to safeguard sensitive data or functionality due to misconfigurations, but is only a partial solution to this issue.
M9: Insecure Data Storage	Verimatrix Anti-Tampering™, plus rooting detection and data protection.
M10: Insufficient Cryptography	Verimatrix Code Shield™ whitebox cryptography secures cryptographic keys by embedding them directly into the app code, making the keys invisible. Secondary detections can be triggered via Verimatrix Anti-Tampering™ or Verimatrix Man-in-the-Middle Interceptor™ if exploited.

Compatibility

Most browsers, JavaScript, frameworks, and libraries across hybrid environments, plus:

- Angular
- EmberJS
- Ionic
- Meteor
- NativeScript
- Next.js
- Node.js
- Nuxt.js
- React
- React Native
- Vue
- Webpack
- HTML 5

About Verimatrix

- French public company (Euronext Paris: VMX).
- 9 worldwide offices, 60+ awards, 151 patents.

EMVCo QUALIFIED · ISO 9001 CERTIFICATION intertek · ISO 27001:2022 CERTIFICATION intertek · HIPAA COMPLIANT · PCI DSS COMPLIANT · PSD2 · GDPR

About Verimatrix Cybersecurity

Verimatrix protects the applications that drive the digital economy. Verimatrix XTD employs advanced obfuscation, anti-tamper, and environmental checks to shield Android and iOS mobile apps from attack. Additionally, its extensive suite of application shielding capabilities spans mobile, embedded, desktop, and web platforms. By harnessing AI and ML for continuous threat intelligence, XTD delivers real-time application risk assessment, empowering organizations to quickly detect and respond to emerging threats, particularly for applications on "unmanaged" consumer devices that are connected but not controlled by traditional IT means.

VerimatrixCybersecurity.com

Verimatrix France
Tel: +33 4 43 905 905

Verimatrix USA
Tel: +1 858 677 7800

Verimatrix Germany
Tel: +49 89 55265 100