Extended Threat Defense from the App to the Enterprise

Expand defenses beyond the traditional perimeter with Verimatrix Extended Threat Defense (XTD).

Verimatrix
XTD

PRODUCT BRIEF

Global
Infosec
Award
2023

POWERFUL & CONVENIENT PROTECTION

Verimatrix XTD secures today's modern enterprise from risks originating from the edge and beyond - multi-vector threats not covered by existing cybersecurity solutions. Using patented zero-code injection technology, app telemetry and AI/ML, Verimatrix XTD protects the most vulnerable and valuable assets that reside in application servers, databases and remote apps. XTD transforms unmanaged devices to pseudo-manageable, preventing hackers from weaponizing billions of connected apps and helping organizations minimize risks and reduce response time.

73%
Of organizations that experienced mobile-related compromise described their compromise as "major"

60%
Of organizations report that they do not have visibility to runtime threats against mobile apps and APIs

45%
Of organizations had recently experienced mobile-related compromise, almost twice as many as in Verizon survey 2021

What Does Verimatrix XTD Uniquely & Conveniently Offer in One Package?

- Monitor all devices running the customer's app
- Identify and block compromised devices
- Identify and block impersonator apps
- Provide real-time risk scoring for each app access
- Detect app vulnerabilities and zero-day threats

ELIMINATE THE BLINDSPOT CREATED BY TODAY'S CONNECTED APPS

SECURE ALL CONNECTIONS
Verimatrix XTD protects the connection between companies and their mobile endpoints. We can seamlessly turn your customer's mobile apps into security control points so that devices that were previously unmanageable are now pseudo-managed.

DEFEND UNMANAGED DEVICES
Transform unmanaged devices into pseudo manageable devices, gaining real-time, continuous threat intelligence utilizing Verimatrix's zero-code telemetry technology.

ATTACK PREDICTION
Comprehensive, predictive analysis of cyberthreats based on large data sets, artificial intelligence (AI) and machine learning (ML), to recognize statistical patterns, making future predictions to benefit the enterprise.

SHIELD APPS & DEVICES
With self-defending mobile application shielding, Verimatrix provides organizations with layers of protections such as obfuscation, environmental checks and anti-tamper, plus 24/7 monitoring with immediate detection when an app is under attack with remote shut-down capability.

ATTACK PATTERN DETECTION
Using behavioral analysis, better understand the threat profile of your installed base of users, and drill down into the risk score of an individual app instance, with real-time notifications of high-risk events to uncover hidden dangers in your enterprise security wall.

SIEM INTEGRATION
Verimatrix XTD has integration capabilities with various security information and event management systems, which allows you to automate your prevent and detect capabilities end-to-end to align with the way you choose to manage your extended threats.

THE TRUE BLINDSPOT SOLUTION: VERIMATRIX XTD

	On-Device Security	Device Remote Visibility & Control	Behavioral Analysis	Number of Devices
Managed Devices	✔	✔	✔	M
BYOD	✖	✔	✔	L
Unmanaged Devices	✖	✖	✔	XL
Connected Apps	(logo)	(logo)	(logo)	XXL

verimatrix
DRIVING TRUST

VERIMATRIX XTD COMPLIES WITH GDPR AND PRIORITIZES PRIVACY

GDPR	EU Cyber Resilience Act	PCI DSS Certification
Law: EU's General Data Protection Regulation sets guidelines for the collection and processing of personally identifiable information (PII).	**Pending Law:** Developers & manufacturers required to secure internet-connected products like mobile apps, conduct risk assessments, and report incidents.	**Law:** Payment Card Industry Data Security Standard. This certificate shows controls are in place around card holder data to reduce credit card fraud.
Solution: Verimatrix XTD helps customers build secure & compliant mobile Apps to secure against PII exposure and theft.	**Solution:** Verimatrix XTD and its award-winning mobile App security meets CRA requirements.	**Solution:** Verimatrix XTD helps customers prove PCI compliance for Visa and Mastercard with strong authentication

XTD RISK SCORING REVEALS ANOMALIES & PATTERNS

APP

| Resigning | Hacking Tool Connecting | Event timestamps | Screen overlay |
| Install source | Code Tampering | Debugger Attaching | Use case data |

DEVICE

Malware	Content	OS (e.g. version and kernel)	Type Allocation Code (TAC)
Emulator / Virtualization	Rooted / Jailbroken	Hardware (e.g. CPU)	Additional Hardware (e.g. inputs & outputs)
Location	Device (e.g. OEM and model)	Developer Mode Enabled	Physical Environment (e.g. lights and movement)

NETWORK

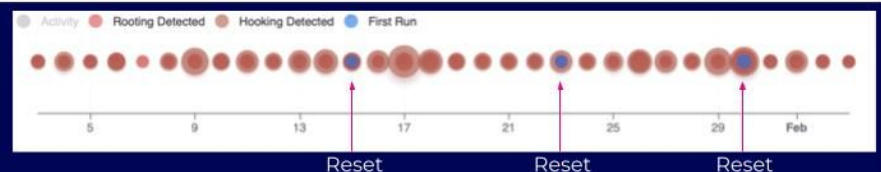| IP Address | Man-in-the-middle | VPN | IP Network trustworthiness |

XTD Vulnerability Database

Verimatrix AI/ML based risk scoring

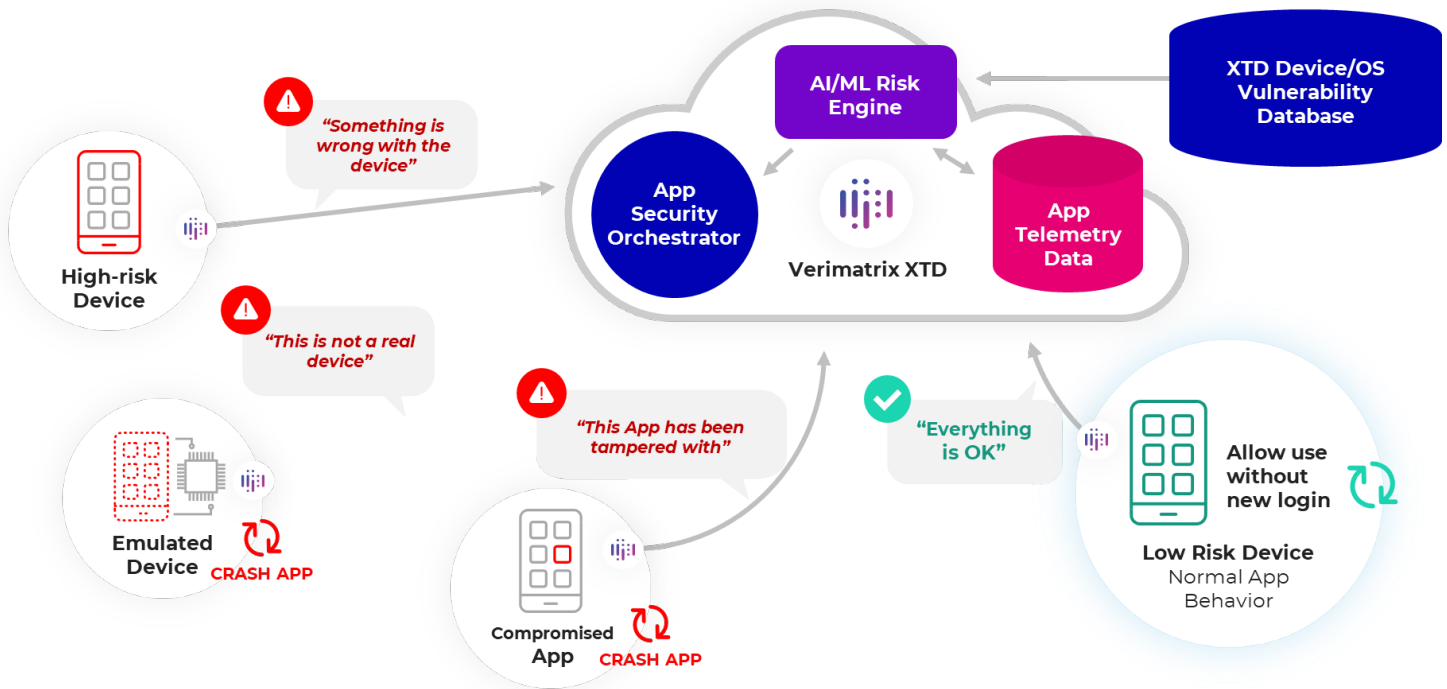**Combined intelligently, data elements reveal true risk profile of every device:**

- **Behavior** – device isn't acting as expected (e.g. never moving).
- **Temporal** – events from the device show a pattern over time (e.g. repeated attaching of debug tools).
- **Environmental** - device and physical attestation (e.g. developer mode, and the ambient light-level does not change).
- **Misalignment** – cross checking data points (e.g. GPS, IP location and cellular network service don't match).
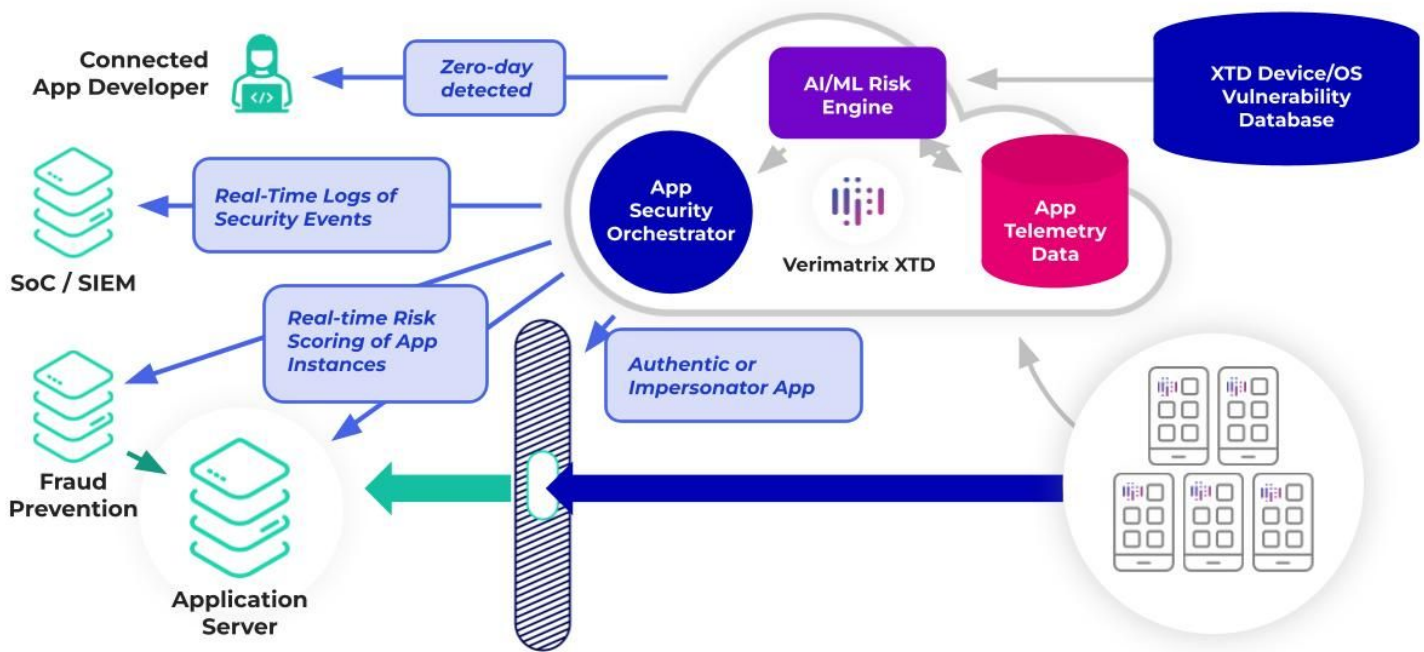
Real-world Example
App is wiped and reset immediately before every kick-off. Verimatrix analysis suggests this is done to prepare the App for abuse. Overlaying this data with behavior data shows reset happens prior to high-value actions. Normal users don't wipe their app periodically.

Activity • Rooting Detected • Hooking Detected • First Run

5   9   13   17   21   25   29   Feb

Reset   Reset   Reset

XTD: MITIGATING THE REMOTE APP RISK

XTD: PROTECTING THE APPLICATION SERVER & DB

XTD's Secret Sauce: Zero-Code Injection Technology

Unprotected Connected App
Easily reverse engineered by attackers to become a vehicle for attack.

Verimatrix App Shield

In-App Protection
Defenses are injected directly into the client app's logic as well as a security agent to connect to XTD.

Hardened Connected App
Protect against reverse engineering and tampering while also providing real-time telemetry to the Verimatrix XTD service.

CONTACT US

About Verimatrix
Verimatrix (Euronext Paris: VMX) helps power the modern connected world with security made for people. We protect digital content, applications, and devices with intuitive, people-centered and frictionless security. Leading brands turn to Verimatrix to secure everything from premium movies and live streaming sports, to sensitive financial and healthcare data, to mission-critical mobile applications. We enable the trusted connections our customers depend on to deliver compelling content and experiences to millions of consumers around the world. Verimatrix helps partners get to market faster, scale easily, protect valuable revenue streams, and win new business.

Verimatrix Headquarters
Impasse des carrés de l'Arc
Rond-point du Canet
13590 Meyreuil , France
Tel: +33 4 42 905 905

Verimatrix USA
6059 Cornerstone Court West
San Diego, CA 92121-3713
United States
Tel:+1 858 677 7800

Additional offices in China, Finland, France, Germany, Netherlands, United Kingdom and the USA. Sales offices located in multiple countries.

verimatrix
DRIVING TRUST