Malware & Forensic Analysis

Replica Isolated Environments

Instant. Secure. Frictionless

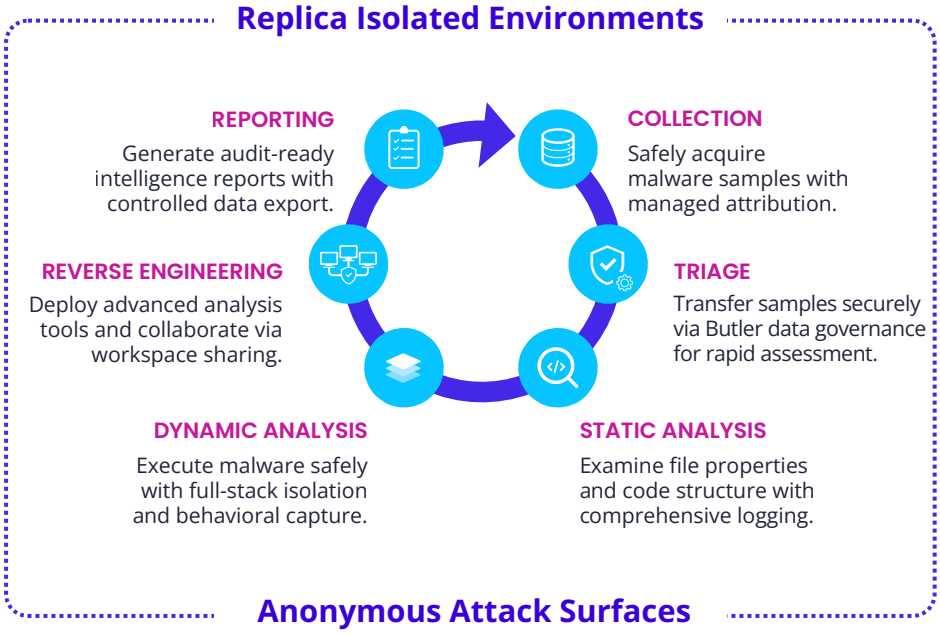
REPLICA
POWERED BY GREY MARKET LABS

Secure, Scalable Infrastructure for Malware Analysis and Threat Containment

As malware grows more sophisticated—leveraging polymorphism, sandbox evasion, and delayed detonation—security teams are under pressure to analyze threats faster, deeper, while protecting core infrastructure. Traditional sandboxing, virtual machines, and burner devices are too slow, too fragile, and too risky. They lack the isolation, speed, and operational fidelity needed for today's high-stakes malware response.

Replica provides ephemeral isolated environments that support safe detonation, reverse engineering, and real-time collaboration without attribution, infrastructure risk, or IT bottlenecks.

- Instant Deployment
- Full Stack Isolation
- Dark Web Access
- Secure Collaboration
- Physical Phone Access
- Audit -Ready Logging



Business Challenge

Closing the Gaps in Malware Analysis Speed and Governance

Security leaders must balance speed, safety, and compliance as malware threats escalate. Yet traditional approaches—VMs, sandboxes, burner devices, and unmanaged IT—are slow to provision, costly to maintain, and lack governance. They create blind spots in oversight, hinder collaboration, and operate outside compliance frameworks. These gaps increase dwell time, elevate breach risk, and make regulatory alignment harder. The business needs a scalable, governed infrastructure to contain malware and act fast without compromise.

Current State Limitations:

- Analysts rely on improvised sandboxes or costly burner device set ups
- Malware C2 servers block access from known analysis infrastructure
- Analyst identity exposure to threat actors compromises investigations
- Sharing live malware samples across teams creates security gaps
- Inadequate forensic logging fails to provide adequate evidence

Replica Isolated Environments

The Solution

Replica delivers fully functional online environments that mirror standard workstations while keeping all activity securely isolated from corporate infrastructure. Replica's patented architecture enables rapid malware detonation and deep forensic analysis, with secure pixel-streamed video ensuring uncompromised fidelity and protection.

The integrated anonymous attack surface gives investigators the freedom to safely interact with malware-hosted infrastructure, enabling attribution-free operations and full protection against tracking.

Key Benefits

Safe Malware Detonation
Run payloads in isolation, no risk to systems.

Advanced Reverse Engineering
Analyze behavior, code, and infrastructure.

Mobile & Cross-Platform Testing
Test mobile, SMS, and 2FA exploits.

Collaborative Forensics
Share workspaces for faster response.

Empowering Malware Analysts

With Replica, every stage of malware analysis—from safe acquisition to forensic reporting—takes place in a rapidly deployed environment designed to eliminate exposure, enable collaboration, and produce audit-ready intelligence.

The Replica Advantage

Infrastructure Protection

Select pre-configured images for cloud, on-prem, or mobile analysis, or create custom images for specific workflows. Physical devices are available for testing mobile-targeted malware like SMS or 2FA exploits.

Tradecraft-Driven Operations

Flexible networking and persona tools enable analysts to appear as anybody-from-anywhere, safely engaging with attacker infrastructure, C2 servers, or delivery channels while maintaining complete identity and location privacy.

Collaboration & Data Governance

The proprietary Butler™ system controls all file transfers—malware in, intelligence out—while maintaining compliance and audit trails. Entire malware environments can be securely shared across teams for collaborative analysis.

Built by Former Intelligence Professionals
Replica was born from decades of cyber counterintelligence experience. Every capability is rooted in operational tradecraft proven in the most sensitive missions.