A.R.M.O.R

Attach Response & Mitigation Of Risk – Platform & Service

REJIS

Anti-Malware | Anti-Evasion | Anti-Hacker + Remote Isolation & Incident Response Triage

REJIS ARMOR uses a low impact agent that runs as a persistent service to protect endpoints, utilizing core capabilities, built-in by Minerva Technology Labs. REJIS ARMOR helps protect systems from attacks that bypass other defenses, including "next-gen" AV tools and app whitelisting. Deployment is fast and simple.

Core Capabilities (Built-in Capabilities of Minerva Technology)

Hostile Environment Simulation	Simulates environments, such as analysis sandboxes, that malware is often designed to avoid. This module deceives the threat into deactivating itself because it "believes" the environment is not safe for it to launch.
Memory Injection Prevention	Blocks attempts by fileless threats to avoid executing code from the file system. For instance, malicious software might hide itself in a legitimate process. This module interferes with injection attempts, causing such malware to exit or crash.
Malicious Document Prevention	Breaks or otherwise disarms malicious documents that try to abuse features such as macros, scripts, and built-in tools. This module allows users to benefit from full capabilities of modern applications without worrying about infections.
Ransomware Protection	Intercepts attempts to destroy documents, placing the protected files into a cache that is maintained on the endpoint. This module allows users to retrieve the affected files without relying on backup solutions or paying the ransom.
Browser Isolation	Protect users from browser-based attacks. This module allows users to benefit from secure browsing.
Process Isolation	The ability to run an untrusted application in a secure way that will not endanger the organization.
Malware Vaccination	Simulates infection markers to deceive malware into "believing" it's already on the system. This module causes the corresponding threat to shut itself down to avoid infecting the same environment more than once.
Living-off-the-Land-Prevention	Interferes with attempts to misuse tools built into the system to cause damage without using classic forms of malware. This module prevents threats from "trampolining" off such tools to infect the endpoint or cause damage.
Critical Asset Protection	Cloaks sensitive files, processes, and other artifacts to prevent attackers or their malware from harvesting credentials (or other sensitive data) even if the threat finds a way to run on the system.
Endpoint Investigator	Collects local process activity to accommodate forensic analysis, threat hunting, and other investigations of the system.
Microsoft Windows Defender Management	Use the Management Console to centrally monitor the state of third-party antivirus (e.g., Windows Defender Antivirus) for Defense in Depth endpoint protection. *can only manage antivirus solutions that post to Windows Security Center. *Windows Defender for Windows Servers cannot be centrally managed at this time.

Call 314-535-1950 | **rejis.org**

*Extended Capabilities: (Capabilities Added to Create REJIS' ARMOR Platform)

Endpoint Isolation

Ability to Remotely Isolate Windows Systems to Contain Malicious Activity. *Linux systems require ssh access from any on network Windows system with an agent installed.

Secure Remote Incident Response

Ability to Open a SECURE Encrypted Tunnel between the isolated/infected workstation or server and Triage Server for performing Incident Response and Forensics Activities. Triage can be performed via shell or full SECURE RDP Connection on Windows Systems.

*Linux systems require ssh access from any on-network Windows system with an agent installed

Enhanced Malicious Process Execution Blocking

REJIS ARMOR Integrates Enhanced Malicious Process Execution Blocking via Threat Research, Analysis and Implementation.

- Windows agents have the Investigator & ALL Protection modules
- Mac agents have the Investigator & Ransomware modules
- Linux agents have the Investigator module

Comparison to Traditional Endpoint Detection & (EDR) Response Platforms

Capabilities	Traditional EDR	REJIS ARMOR
Endpoint Isolation	Few/Minimal	✓
Remote IR	Few/Shell Only	Full Shell and RDP
Endpoint Malware Vaccination	X	✓
Augment's baseline security controls	X	✓
Assists with containing malware outbreaks	✓	✓
Supplies details about evasion attempts	Some	✓
Designed for in-depth post-incident investigations	Some	✓
Prevents environment-aware threats	X	✓
Prevents the misuse of document features	X	✓
Prevents memory injection and other fileless threats	X	✓
Provides end-to-end anti-ransomware solution	X	✓
Operates automatically and Sandboxes Threats	X	✓
Enhanced Malicious Process Execution Blocking	X	✓
Protects Against Zero-Day Attacks & Supply Chain Compromise	Minimal	✓

Call 314-535-1950 | **rejis.org**