MINERVA

Minerva Anti-Evasion Platform

Block Unknown Threats That Are Designed To Evade Your Existing Defenses

Minerva Anti-Evasion Platform automatically blocks attacks that are designed to evade your existing security defenses. Instead of attempting to seek and identify malware, Minerva creates a virtual reality on the endpoint that causes malware to disarm itself. This unique approach allows enterprises to stop unknown, advanced malware prior to engaging costly investigative and recovery resources.

SOPHISTICATED ATTACKS ARE DESIGNED TO EVADE YOUR DEFENSES

Despite the continued investments in security solutions, endpoints are still being infected with advanced malware. Developing sophisticated malware takes time and requires heavy financing. Malware authors often design and test their creations to remain unnoticed to existing security tools, to derive maximum value from their malicious software. Such evasive malware avoids detonating in sandboxes or forensic environments, hides in memory of legitimate processes, employs scripts and document files, and relies on other techniques that bypass traditional and next-gen security measures.

To combat these threats, enterprises continue to rely on their existing endpoint protection and detection systems. Though these solutions implement various methods to safeguard systems, their core techniques are grounded in mechanisms that attempt to identify malware based on previously-seen malicious programs. Such approaches, whether they employ signatures, machine learning models or behavioral footprints, inevitably miss evasive malware that's designed to deviate from the earlier, known patterns. As a result, organizations find themselves chasing after alerts and investigating incidents, many of which turn out to be false positives, yet end up failing to block unknown attacks that employ evasive techniques.

DON'T JUST ASSUME THE BREACH. PREVENT IT.

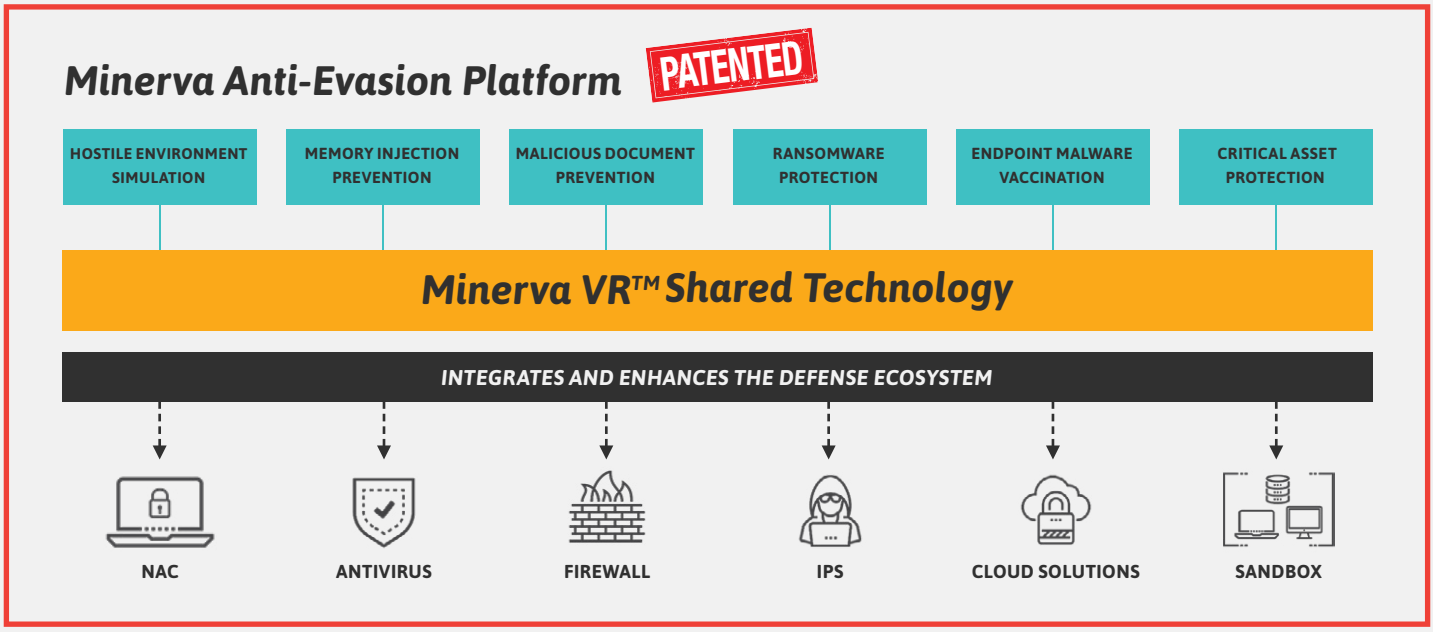
Realizing that current security measures are not enough to keep endpoints protected, enterprises struggle to decide between the costly option of replacing existing anti-malware solutions with new ones that promise better protection, or adding yet more products that demand additional resources. In both cases, unknown evasive malware will only be detected after the breach occurs.

CREATING AN ENVIRONMENT WHERE MALWARE DISARMS ITSELF

Minerva is focused on preventing unknown threats that are designed to evade existing defenses without attempting to seek and identify malware.

This unique approach to blocking unknown evasive threats, avoids duplicating the methods employed by other endpoint security technologies, supplementing baseline anti-malware solutions to address the weakness inherent to any detection-based approach.

Minerva Anti-Evasion Platform is built upon the patent-pending Minerva VR™, which controls how malicious software "perceives" its environment on the endpoint, allowing Minerva to deceive malware in a way that neutralizes threats in a manner drastically different from your existing security layers.



Minerva Anti-Evasion Platform boosts customers' endpoint defense posture against unknown, evasive threats with several modules, which reinforce each other to form a powerful centrally-managed solution:

Hostile Environment Simulation uses the core strength of evasive malware against itself. The nature of evasive malware is to query its environment to ensure it is not caught by the enterprise security systems. Minerva's response deceives the malicious program into believing the environment is not safe for it to launch in. This results in the malware suspending or terminating its execution.

Memory Injection Prevention blocks attempts by fileless malware and other stealthy malicious software to hide in a legitimate process, preventing malicious programs from gaining a foothold on the endpoint and rendering such evasive techniques ineffective.

Malicious Document Prevention blocks malicious actions initiated by document files, such as those that employ macros, PowerShell and other scripts. Minerva Anti-Evasion Platform allows enterprises to utilize full capabilities of modern document files while preventing damage that malicious versions of such files might cause.

Ransomware Protection intercepts attempts by destructive malware to encrypt or delete documents and backs up the original files on the fly. Minerva Anti-Evasion Platform then provides the user the option to retrieve the file for immediate restoration without relying on other backup solutions or OS capabilities to ensure the safety of important files and avoid paying the ransom.

Endpoint Malware Vaccination exploits a typical behavior of many malicious programs that avoid infecting the same system more than once. By simulating the infection marker that the specimen uses to determine whether it's already on the endpoint, Minerva Anti-Evasion Platform blocks the attack by causing malware to avoid infecting the system.

Critical Asset Protection blocks malware from interfering with critical assets on the endpoint. By hiding or restricting access to such applications and their artifacts from malware, Minerva Anti-Evasion Platform prevents threats from damaging or stealing sensitive data, such as password vaults, cached logon credentials, Personally-Identifiable Information (PII) or other business-critical information.

KEY BENEFITS

Block Unknown Evasive Attacks
Prevent attacks that get past existing defenses with a radically different approach to strengthening endpoint security.

Low Admin Overhead
Free resources from complex deployments, heavy ongoing maintenance and avoid re-imaging.

No Business User Impact
Strengthen security without slowing down or inconveniencing end-users.

Avoid Costly Replacements
Strengthen endpoint defense without the risks and costs of rip-and-replace projects.

FINALLY, ENDPOINT SECURITY THAT DOESN'T ADD OPERATIONAL BURDEN

To ensure extremely low operational burden, Minerva Anti-Evasion Platform is a passive solution that doesn't engage in any actions that might drain the system's performance, cause false alarms or interfere with legitimate applications. Deployed as a unified installer, it leaves a minimal footprint and requires no reboots or pre-requisites.

Minerva Anti-Evasion Platform also alleviates the operational burden of alert overload. Resources no longer need to waste time on meaningless alerts as only real events are prevented, resulting in an extremely low rate of false positives.

Easy Deployment
As a super-thin agent, Minerva can be installed on thousands of machines in no time and without reboots.

Effective in Offline Mode
Minerva doesn't depend on live or periodic updates and thus remains effective even when endpoints are disconnected from the enterprise network.

Reduce the Re-Imaging Burden
Minerva prevents damage from every type of evasive malware or ransomware, blocking it before install.

No False Positives
Once a Minerva notification appears, you know that a real threat was neutralized and prevented before any damage has been done.

Lightweight
As Minerva doesn't have a heavy agent and performs no active scanning, we have no impact on the endpoint's performance.

No Maintenance Burden
Minerva doesn't require ongoing upkeep to operate at its best. It even updates itself automatically with new capabilities on a regular basis.