MINERVA

Solution Brief

Minerva Safeguards VDI Environments from Unknown Threats

Attacks that Evade Defenses

Despite the continued investments in security solutions, endpoints are still being infected with malware. The authors of malicious software often design and test their creations to remain unnoticed to existing security tools, so they can derive maximum value from their creations. Such evasive threats avoid detonating in sandboxes or forensic environments, hide in the memory of legitimate processes, employ scripts in document files, and rely 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.

Solution Overview: Causing Malware to Disarm Itself

Minerva protects enterprises from threats that are designed to evade existing defenses by controlling how malware perceives its environment. This innovative approach causes malicious software to disarm itself before it can cause damage, freeing organizations from having to engage in costly and risky post-incident activities.

The lightweight nature of Minerva's Anti-Evasion Platform makes it highly effective for safeguarding Virtual Desktop Infrastructure (VDI) environments, protecting not only the underlying VDI server, but also securing individual virtual desktops.

Minerva's Anti-Evasion Platform prevents unknown threats that are designed to evade existing defenses without attempting to seek and identify malware. Minerva's techniques for blocking unknown evasive threats, avoid 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's solution is comprised of several modules that reinforce each other to form a powerful centrally-managed approach to boosting defenses against previously-unseen, evasive threats:

Highlights

- *Prevent threats that use evasive techniques that bypass traditional and next-gen security measures.*
- *Supplement baseline anti-malware solutions to address the weakness inherent to any detection-based approach.*
- *Enhance VDI security by introducing powerful anti-malware capabilities to every virtual desktop without being concerned about performance or operational overhead.*

- **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's 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's 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 avoidinfecting 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's 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.

Solution Integration: Uniquely Suited for Securing VDI

Minerva's Anti-Evasion Platform is VMware Ready certified, having introduced official support for safeguarding VMware Horizon VDI environments from malicious software. Given the lightweight nature of its agent, this allows Minerva to enhance VDI security without adding any performance overhead to customers' VDI solutions.

Minerva's architecture allows customers to deploy our agent on the VDI host server as well as inside the individual virtual machines, providing reliable anti-malware protection for every VDI user with no prerequisites. As a result, the individual VDI virtual machines will remain protected even against threats that cannot be seen from the underlying VDI server. VMWare Horizon customers also benefit from being able to easily deploy Minerva Anti-Evasion Platform agents to 32 and 64-bit versions of Microsoft Windows by using a single installation package.

By adding Minerva to their VDI solution, enterprises can introduce powerful anti-malware capabilities to every virtual desktop without being concerned about performance or operational overhead. In contrast, other endpoint security solutions often require customers to disable key functionality to safeguard each virtual machine or can only run on the underlying server.

About Minerva

Minerva is an innovative endpoint security solution provider that protects enterprises from today's stealthiest attacks without the need to detect threats first, all before any damage has been done. Minerva Anti-Evasion Platform blocks advanced threats designed to evade existing defenses, by creating a virtual reality that controls how malware perceives its environment. Without relying on signatures, models or behavioral patterns, Minerva's solution causes malware to disarm itself, thwarting it before the need to engage costly security resources.

Headquartered in Israel, and with offices in New York and Atlanta, Minerva boost customers' existing defenses without the need to embark upon a costly and risky overhaul of their entire endpoint security architecture. To learn more about Minerva, visit **www.minerva-labs.com.**