



## Prevent Outbreaks & Contain Threats by Simulating Infection Markers on Endpoints

Malicious programs often leave infection markers on the endpoint to avoid infecting it twice and risk operational issues and detection. Defenders can use this behavior to their advantage by mimicking the presence of the markers to vaccinate endpoints from the associated threats. Minerva is the first company that offers the ability to deploy infection markers in a manner suitable for real-world production deployments across the enterprise.

Minerva's Endpoint Malware Vaccination, part of the patented Anti-Evasion Platform, enables enterprises to immunize endpoints in moments by simulating infection markers to deceive the malware into believing it has already infected the system. This innovative approach allows Minerva's customers to prevent infections and neutralize attacks, even if other defensive capabilities were unable to block the attack.

Minerva's ability to simulate (rather than actually create) infection across all enterprise endpoints markers allows it to be highly selective regarding how and when it reveals the presence of the vaccine. This allows Minerva's customers to vaccinate endpoints without cluttering the system with unnecessary artifacts, without interfering with legitimate applications and without affecting the end-user.

## Contain Malware Outbreaks in Moments.

When combatting malware that utilizes infection markers, incident response and threat hunting teams can contain an active outbreak using the infection marker even if baseline anti-malware tools do not prevent the infection.

After determining the infection marker by analyzing the malware or by relying on third-party threat intelligence, the organization can use Endpoint Malware Vaccination to rapidly deploy the vaccine to contain the outbreak, preventing variants of this malware family from infecting additional systems.

Minerva's centrally managed approach to vaccination provides enterprises a quick and hassle-free way to gain control and contain outbreaks based on the following advantages:



### No Impact on End User

Operates without using system resources that impact machine performance.



### Immediate Alert to a Threat Prevented

Monitors access to all simulated artifacts, reporting to the central console and to other security solutions for increased effectiveness.



### Broad Coverage

Simulates the specified infection marker regardless of the attack vector or exploit being used to execute it (even for fileless attacks).



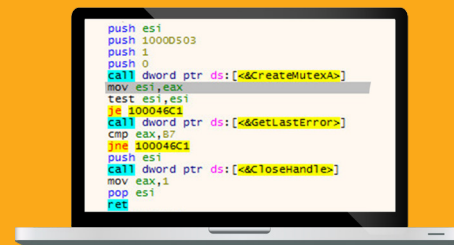
### Ease of Deployment & Management

Distributed in moments even across large enterprises, for new as well as old legacy systems.

## Always in Control – Get Ahead of Global Malware Attacks

Enterprises can also use Endpoint Malware Vaccination to preemptively vaccinate systems during global malware outbreaks. Organizations especially concerned of specific threats in the wild that have been publicized or updated in their threat intelligence platform can apply infection markers to prevent infection before the specimen finds its way into the enterprise.

In its current version, Minerva supports commonly-seen infection markers that use mutex objects. Minerva plans to expand its vaccination capabilities to other types of markers, including those that utilize files and registry keys, in the upcoming product releases.



## Immunizing Against WannaCry

*When a global malware outbreak occurs, you can use Minerva's Endpoint Malware Vaccination to preemptively vaccinate all your endpoints against the threat. For example, companies could have vaccinated themselves against variants of the highly-prolific WannaCry worm by defining a mutex-based infection marker releases.*

### 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](http://www.minerva-labs.com).**