MINERVA

MINERVA'S PROTECTION CAPABILITIES FOR ENTERPRISES AND INTEGRATION PARTNERS

Minerva is a multi-layer endpoint security solution built on complete prevention of threats at the earliest and most critical stage of an attack – often months before other solutions can even detect them.

Current detection and response approaches require your system to be infected before they can respond and stop the attack, often after some critical damage has already been done. Instead of trying to identify threats by looking for patterns, our patented Simulation Engine breaks the attack chain and prevents the attacks before they can even get started.

Minerva's solutions augment existing capabilities of our enterprise customers and integration partners, strengthening the entire security ecosystem.

This short whitepaper explains how:

- The Minerva Simulation Engine forms the unique and practical core of our approach.
- Minerva builds upon the Simulation Engine to stop infections that bypass other defenses.
- You can use Minerva's solutions to protect systems from a range of attacks.
- Minerva's approach safeguards systems and devices against modern threats.

The Minerva Simulation Engine: Perception Control

The Minerva Simulation Engine is the core of our technology for protecting systems by controlling how applications perceive their environment. The context-aware nature of this patented approach allows Minerva to:

- Simulate what's not actually there

  for example causing malicious software to shut itself down by making it "think" it's running in an analysis sandbox.

- Hide or protect what's there

  for example concealing sensitive files or processes to prevent the attacker from accessing sensitive data.

- Restrict malicious execution flows

  for example breaking the attack chain that attempts to misuse built-in tools to compromise the endpoint.

- Interfere with exploits and injection attempts

  which aim to run malicious code inside trusted applications to evade detection.

- Gain visibility into local activities

  for example investigating a potential incident to determine the nature of the attack.

We use these core capabilities to build a variety of modules that work together to safeguard a variety of endpoint categories — laptops, servers, ATMs, printers, mobile devices, and more — from threats that are impractical, costly, or resource-intensive to stop using other methods.

Minerva’s Modules: Stop What Others Miss

Building upon the Minerva Simulation Engine, our modules fit together according to the needs of our enterprise customers and integration partners. Minerva’s catalog includes the following capabilities, which cover the gap left by other security measures without overlapping with them:

Module	Description
Hostile Environment Simulation (HES)	Completely controls how processes perceive their environment. With HES, we can make processes think they are in a position of weakness which will lead to detection, such as an analysis sandboxes. Most malwares are designed to avoid these situations in order to prevent detection, and HES can deceives them into deactivating as they “believes” the environment is not safe for deployment.
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 or encrypt documents, placing the protected files into a cache that Minerva maintains on the endpoint. This module allows users to retrieve the affected files without relying on backup solutions or paying the ransom.
Browser Isolation	This module allows users to benefit from secure browsing by isolating the browser from the rest of the system, preventing it from spawning malicious processes or gaining access to secure and sensitive documents.
Process Isolation	The ability to run an untrusted application in a secure way that won’t endanger the organization by isolating it from the rest of the system, and preventing it from spawning malicious processes and gaining access to sensitive documents.

Module	Description
Malware Vaccination	Simulates infection markers to deceive malware into "believing" it's already on the system, shutting itself down to avoid infecting the same environment more than once. Infection marker simulation can detect a query made by an attacker and simulate wildcard markers to cover a wide range. For example, simulate the existance of *wannacry* markers.
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 make them invisible to attackers or their malware who want to harvest credentials (or other sensitive data) or manipulate key files, 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. This module also provides visibility into the security posture of the endpoint.
Antivirus Orchestration	Use Minerva's centralized management capabilities to monitor, configure, and remediate the state of third-party antivirus (e.g., Windows Defender Antivirus) that form the basis of your endpoint protection.

These modules work together to reinforce each other. Minerva can provide them as part of a single, unified solution to its enterprise customers. We can also make them available à la carte to integration partners who seek to expand their own products.

Minerva's Solutions:
Eliminate the Endpoint Security Gap

Our modules, powered by the Minerva Simulation Engine, form the basis of several Minerva solutions that eliminate the endpoint security gap in a variety of scenarios.

They include:

[Minerva's Anti-Evasion Platform

Dramatically strengthen the anti-malware posture of Windows-based endpoints by causing malware to disarm itself if it attempts to evade antivirus tools or analysis sandboxes. The harder the attackers try to bypass detection, the more effective the solution becomes. Enterprises benefit from more secure and stable endpoints without performance overhead or false positives by adding this solution to their existing baseline antivirus toolset.

[Minerva's End-to-End Endpoint Protection

If using Microsoft Windows, benefit from the cost-effective model of Windows Defender Antivirus while using Minerva to manage this baseline antivirus solution while also taking advantage of Minerva's unique and advanced capabilities. In addition, using Minerva's features such as Malware Vaccination and Endpoint Investigator to quickly investigate and contain threats throughout the enterprise.

[Malware Protection for ATMs

Safeguard against jackpotting and other malware-enabled attacks on ATMs, even if the threat bypasses other security controls. Minerva's unique approach cloaks ATM middleware components, so that only legitimate ATM applications can interact with cash-dispensing and related hardware devices. This capability works together with the other relevant Minerva modules to interfere with evasion tactics. Once Minerva prevents the attack, it notifies the organization, allowing it to respond right away.

Remote User Protection

Provides enterprise grade endpoint security on perconal unmaged (BYOD) devices owned by employees or third parties, automatically only when the user connects to the company VPN or EDI, protecting both sides from malicious attacks, keyloggers, screenshotting etc. without compromising any of the 3rd party’s privacy.
This install-free just-in-time solution automatically validates the endpoint’s state before allowing it to connect to enterprise assets, and can terminate the connection if the system is deemed infected.

Minerva for Sandbox Extension

By integrating with the customer’s or integration partner’s malware analysis sandbox, Minerva significantly increases the tool’s conviction rate. We do this by reporting upon the sample’s evasion attempts, causing malware to self-convict and allowing the sandbox to detect sandbox-aware and other advanced threats. Minerva can also use the sandbox to automatically generate infection markers that enterprises can use as “vaccines” against the corresponding malware families.

Minerva SDK for Integration

Integration partners can include Minerva’s unique capabilities in their own solutions to defend against evasive and other advanced threats without overlapping with their solutions’ existing features. Minerva can supply the modules to address relevant risks, allowing the partner to interact with our components through an extensive set of APIs. The integration can take place on each system using our plugin architecture, or on the back-end via centralized management technologies.

Minerva’s unique approach allows you to disrupt attacks that would normally bypass other security controls. Our lightweight technology can protect not only modern systems, but also legacy endpoints that are low on resources and that struggle against today’s threats.

Our endpoint safeguards save enterprises time and money that would otherwise be spent investigating incidents and recovering from breaches. And our modular design allows customers and partners to use Minerva-provided solutions or customize their Minerva deployment to fit their existing defense architecture.

Minerva’s Safeguards for Systems

Minerva’s Anti-Evasion Platform protects servers and workstations from threats that normally bypass other security measures. We accomplish this without scanning any files or processes. Instead, we rely on the Minerva Simulation Engine to selectively conceal or reveal relevant artifacts or otherwise deceive malware, causing it to fail to reach its objective.

For example:

- By simulating the presence of security tools or analysis sandboxes, Minerva causes many evasive malicious programs to terminate themselves, because they’re designed to avoid such “hostline” environments. For an illustration, see UIWIX ransomware.
- By limiting the ability of malicious documents to interact with tools such as PowerShell or other utilities that enable living-off-the-land attacks, we allow enterprises to use modern documents without fear. For an illustration, see Emotet downloader.
- By concealing sensitive information and other local components targeted by data stealers, Minerva protects critical assets on the system, including sensitive configuration files, memory contents of POS systems, cached login credentials, and more.
- By intercepting attempts to inject malicious code into processes, Minerva causes exploits and in-memory to attacks fail, forcing the malicious process to exit or crash. For an illustration, see AZORult information stealer.
- By redirecting activities that destroy local files, we protect endpoints from losing documents even if ransomware bypasses other measures. Minerva tricks ransomware into backing up the files to a local cache, so the victims can easily recover them without paying ransom.

Minerva can offer these and other countermeasures by working alongside customers’ existing anti-malware tools without overlapping or interfering with their capabilities. As a result, the enterprise covers the gap inherent to any detection-focused anti-malware approaches.