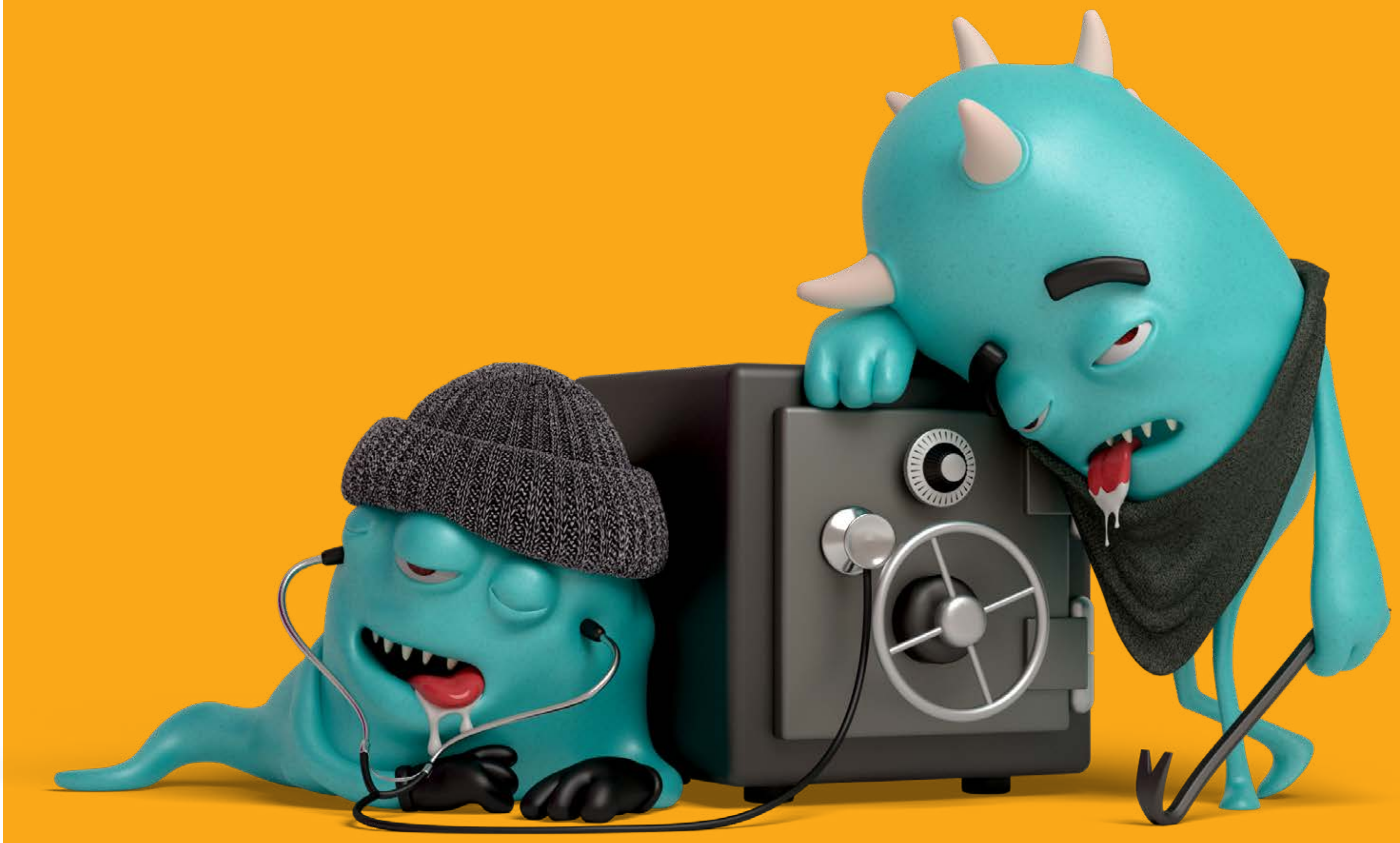
MINERVA McAfee™

McAfee and Minerva Labs

Advanced, Evasion-Proof Endpoint Defense



McAfee® Endpoint Security augmented with the Minerva Anti-Evasion Platform delivers significantly broader threat coverage than any other solution on the market, while boosting endpoint performance.

THE BUSINESS PROBLEM

For as long as there will be anti-malware products, there will be malware designed to bypass them. The evolution of anti-malware approaches is driving adversaries to design malicious software that stays under the radar of security vendors and slips past existing defenses and detection systems. Evasive malware avoids detonating in sandboxes, resides in memory of legitimate applications, employs scripts and document files, and relies on other techniques that bypass traditional and “next-generation” security measures.

MCAFEE AND MINERVA LABS JOINT SOLUTION

By integrating McAfee Endpoint Security and McAfee ePO software with the Minerva Anti-Evasion Platform, cyberdefenders gain significantly improved endpoint protection against both evasive and non-evasive malware and single-pane-of-glass visibility, where all events can be monitored via McAfee ePO software and new threat intelligence on infections prevented by Minerva. This combination delivers powerful, evasionproof endpoint protection, reinforcing the notion that complementary security approaches, when integrated, are better together.

The Minerva Anti-Evasion Platform causes malware to disarm itself when it attempts to take evasive actions, deceiving the malware about its environment to prevent the attack. In fact, the more advanced the attack, the easier for Minerva to block it. When Minerva is deployed alongside McAfee Endpoint Security, adversaries are forced to pick their poison. Either they implement evasive tactics and get stopped by Minerva, or McAfee security mechanisms will intervene.

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

Hostile Environment Simulation: Simulates the presence of an environment that evasive malware is designed to avoid, such as sandboxes, antivirus, and other anti-malware tools, and, as a result, causes malware to terminate itself.

Memory Injection Prevention: Blocks attempts by fileless threats to hide malicious code in legitimate processes, causing the malware to exit or crash.

Malicious Document Prevention: Disarms malicious documents that try to evade detection by employing macros, PowerShell, and other scripts. Enterprises can utilize the full capabilities of modern documents, while preventing damage that malicious versions might cause.

Ransomware Protection: Intercepts attempts by destructive malware to encrypt or delete documents and backs up the original files on the fly into a cache that Minerva maintains on the endpoint.

Endpoint Malware Vaccination: Simulates infection markers that malware leaves behind in order to not infect the same machine twice and risk being detected. As a result, the malware avoids infecting the system, and the attack is prevented.

Critical Asset Protection: By hiding or restricting access to critical assets on the endpoint, Minerva prevents threats from damaging or stealing sensitive data, such as password vaults, cached logon credentials, personally identifiable information (PII), or other business-critical information and peripheral devices.

McAfee and Minerva integration features:

- Deploy Minerva via McAfee ePO software for all Microsoft Windows operation systems (Windows XP or above, including servers). No reboot is required for installing, upgrading or uninstalling the agent.
- Centrally monitor and feed new threat intelligence of all evasive threats prevented by Minerva through McAfee ePO software.
- Strengthen your security posture by using information from Minerva-prevented threats on the endpoint to enrich the data available to McAfee products within the enterprise.
- Increase the effectiveness of McAfee Data Loss Prevention by blocking malware hiding inside legitimate Microsoft Office documents.
- Vaccinate endpoints with Minerva by simulating the existence of infection markers that McAfee® Active Threat Defense derived.

Operational advantages of Minerva and McAfee when deployed together:

Easy Deployment and Maintenance
Minerva can be deployed through McAfee ePO software without the need for pre-configurations or 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.

Lightweight
Without performing any active scanning on the endpoint, Minerva prevents infection at a very early stage, improving overall endpoint performance when other solutions are

Challenges

- *Effective endpoint defense against evasive threats*

McAfee Solution

- *McAfee ePO*
- *McAfee® Enterprise Security Manager*
- *McAfee Endpoint Security and McAfee® VirusScan®*
- *McAfee® Threat Intelligence Exchange (planned future integration)*
- *Data Exchange Layer (planned future integration.*
- *McAfee® Data Loss Prevention (requires both products to be installed on the endpoint via a single McAfee ePO agent)*
- *McAfee® Advanced Threat Defense (planned future integration)*

Results

- ***Evasion-proof protection:** Prevent infections that use evasive techniques to protect endpoints, without duplicating security approaches.*
- ***Endpoint security across heterogeneous systems:** Strengthen endpoint security via a single agent for modern and legacy versions of Windows, with no prerequisites or reboots.*
- ***Improved endpoint performance:** Minerva doesn't actively scan to prevent malware infections keeping computer resource utilization very low (0.01% CPU; 25MB RAM).*
- ***Easier management:** Deploy Minerva across the McAfee ePO software environment without separately managing yet another endpoint agent, and centrally monitor all endpoint events through McAfee ePO software.*
- ***New threat intelligence:** Avoid changing McAfee ePO-based workflows while adding visibility into evasive threats.*

About Minerva

Minerva is an award-winning, 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's Anti-Evasion Platform prevents malware attacks that evade existing defenses. It does this by deceiving the malware and controlling how it 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. By augmenting your endpoint protection platforms with Minerva, you gain increased coverage and effective prevention against the most sophisticated attacks. Headquartered in Israel, with offices in New York and Atlanta, Minerva boosts customers' existing defenses without the need to embark on a costly and risky overhaul of their entire endpoint security architecture. To learn more about Minerva, visit www.minerva-labs.com

About McAfee ePolicy Orchestrator Software

McAfee ePO software is the industry-leading security and compliance management platform. With its single-agent and single-console architecture, McAfee ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.

About McAfee Data Loss Prevention

McAfee Data Loss Prevention software delivers the highest levels of protection for sensitive data, while greatly reducing the cost and complexity of safeguarding business-critical information. McAfee data protection is delivered through the McAfee ePO platform, for streamlined deployment, management, updates, and reports.

About McAfee Enterprise Security Manager

McAfee Enterprise Security Manager—the foundation of the security information and event management (SIEM) solution family from McAfee—delivers the performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

About Data Exchange Layer

The Data Exchange Layer communication fabric connects and optimizes security actions across multiple vendor products, as well as McAfee-developed solutions. Enterprises gain secure, real-time access to new data and lightweight, instant interactions with other products.