MINERVA

Ransomware Protection

Minerva blocks unknown threats on enterprise endpoints without relying on prior knowledge about malicious programs' patterns or behavior. The Minerva Anti-Evasion Platform accomplishes this by rendering malicious code ineffective by carefully controlling how malware "perceives" its environment. This approach is especially powerful at protecting against unknown ransomware by blocking infections and preventing users' files from being affected.

Minerva stops ransomware by using a combination of innovative capabilities that build upon the company's patent-pending technology: Minerva VR™. Minerva simulates an environment in which unknown malware "decides" to refrain from executing in, and as a result prevents malicious actions before detection and before they cause damage.

Deceiving Ransomware into Terminating Itself

Criminals that develop destructive malware have strong incentives to safeguard their creations from detection for as long as possible. Prior to deploying their malicious programs into the wild, they test whether the files will be flagged by antivirus tools, repackaging them to evade detection. To continue staying under the radar of security products, ransomware often checks whether it's running in a sandbox or otherwise hostile environment before deciding to infect the system.

Minerva Anti-Evasion Platform simulates an environment that ransomware sees as inhospitable, making it look like the very tools that ransomware wishes to avoid are present on the endpoint. This causes evasive malware to halt execution before infecting the endpoint.

Blocking Memory Injection

Another way in which ransomware often attempts to evade detection involves injecting malicious code into legitimate applications or OS components. This approach allows malware to get around security mechanisms such as traditional antivirus, application whitelisting and personal firewalls. Memory injection is often used by malware that is sometimes considered fileless, because in such attacks, adversaries refrain from placing recognizable malicious code on the file system.

Minerva Anti-Evasion Platform interferes with the activities of fileless or other malicious programs that attempt to inject code into other processes, preventing ransomware that uses this evasive measure from infecting the system.
This is yet another layer that contributes towards Minerva's ability to protect systems from ransomware.

Malicious Document Prevention

Ransomware often finds its way onto endpoints by way of Microsoft Office documents, which victims might receive as email attachments. These files can include macro code, which is designed to infect the system when the victim opens the document and enables macros. Such attacks have been exceedingly effective, in part because business users frequently share Microsoft Office files, and in part because it's notoriously difficult to distinguish between legitimate and malicious documents using traditional antivirus approaches.

Minerva Anti-Evasion Platform protects the organization from ransomware that spreads via malicious documents by blocking actions initiated by documents that employ macros, PowerShell and other scripts. This allows Minerva to prevent the infection while allowing the enterprise to continue using macros for legitimate business purposes.

Ransomware Remediation

Should the various security layers fail at blocking ransomware from running on the system, Minerva Ransomware Protection remediates the damage caused by destructive malware. Organizations can restore the encrypted files without relying on backup capabilities such as shadow copies or snapshots, that can easily be disabled by the ransomware or might not even be enabled in the first place.