MINERVA

Prevent Ransomware Before it even Starts.

The First Solution Dedicated to Mitigating the Risk Associated with Ransomware, Co-Existing with other EDR/EPP/XDR Solutions Without Degradation to the Endpoints

Gartner COOL VENDOR 2020

10 Times CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2020

7 Granted Patents

Prevent Both Known and Unknown (Zero-day) Attacks Before They Start, Regardless of Your Team's Size and Skillset.

Minerva's multi-layer anti-ransomware solution is built to completely prevent ransomware 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, usually 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, adding a crucial layer to any security stack.

NEVER PAY RANSOM

Ransomware is built to remain undetected

95% of threats are built to bypass your security. The longer they can remain undetected, the more they can encrypt

Prevention is better than detection

By the time the ransomware is detected, the damage has already been done.

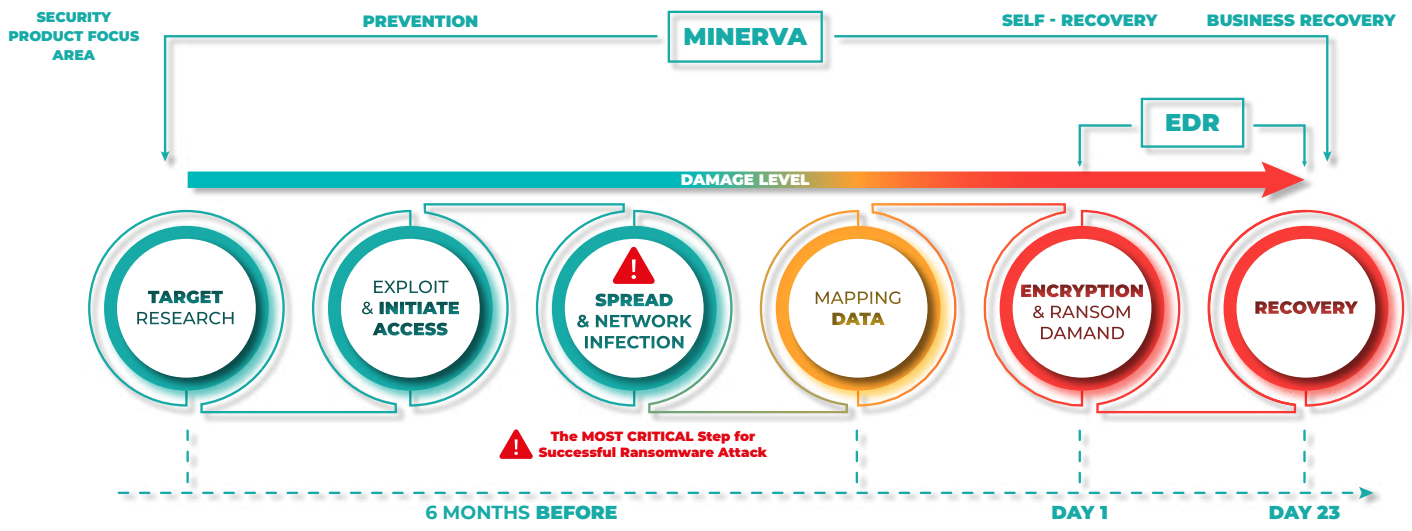
2 Click Installation, Zero-Touch & 100% Autonomous

Rapid Deployment, No prerequisites, No reboots CPU < 1%, RAM < 25MB

Any Platform

For Workstations, BYOD, Legacy Systems and OT/IOT

Ransomware Attack Chain - High Level



MINERVA

Gartner COOL VENDOR 2020

Minerva's Hostile Environment Simulation

Completely controls how processes perceive their environment. With HES, we turn the malware's evasive properties against itself by convincing it that it is about to be detected by a local security measure, forcing it into hiding in order to "remain undetected", which effectively causes it to never deploy.

Blocking malicious macros and powershell attacks

Minerva's Platform blocks ransomware that spreads via malicious documents. This methodology prevents documents from spawning malicious script driven attacks (macros, Powershell etc.), while still allowing the organization to use these processes for legitimate business purposes.

Blocking Memory Injection

Ransomware often evades detection by injecting malicious code into legitimate applications or OS components. This approach allows malware to get around traditional security mechanisms such as antivirus, application whitelisting and personal firewalls. Minerva's memory injection module prevents all fileless attacks from taking place before they even start.

Ransomware Remediation

When other security solutions fail at blocking ransomware from running on a system, Minerva Ransomware Protection remediates the damage caused by destructive malware. With Minerva, organizations can easily restore encrypted files without relying on backup capabilities such as shadow copies or snapshots, that are often disabled by the ransomware or might not even be enabled in the first place.