MINERVA

Solution Brief

Remote User Protection

Modern enterprises increasingly rely on a distributed workforce, with contractors, employees and other users connecting remotely over VPN. In many cases, these individuals access sensitive resources from systems whose security configuration the enterprise does not directly control. This might be because they are user-owned devices or because they're owned by another organization. In these scenarios, the enterprise still needs to take reasonable precautions regarding the security posture of the connecting system. Minerva Labs offers an effective solution for such scenarios.

Remote User Protection enables malware-free VPN connections, protecting enterprises from attacks upon initiation of, or during a remote connection.

Anti-Malware Safeguards for Remote Users

Minerva's Remote User Protection software helps enterprises safeguard themselves from potentially-infected systems connecting over a VPN. It accomplishes this by integrating with the organization's VPN software to initiate a scan of the remote system's processes for known malware before allowing the connection to be established. If the system has active malware, Minerva's transient agent will not allow it to connect. This approach reinforces other security mechanisms that might exist on the remote system without conflicting with other security tools or interfering with the user's day-to-day activities.

Remote User Protection not only safeguards the enterprise from infected systems at the onset of the VPN connection, but also provides controls in case the user's system gets attacked during the VPN session. Even if the system was deemed malware-free when initiating the VPN connection, Minerva's solution interrogates every new process launched on the user's system to determine whether it's recognized as a malicious program, in which case Minerva severs the risky connection.

Remote User Protection is a lightweight agent that activates when the user attempts to initiate the VPN connection without requiring the user to reboot and without interfering with other security tools or software on the system. Once active, it performs cloud lookups of existing or new processes to detect known malicious programs. If the solution spots malware, it alerts the user and terminates the VPN connection or avoids initiating the connection in the first place. The service is automatically disabled when the user disconnects from the VPN session.

Works with Minerva's Anti-Evasion Platform

While Remote User Protection is designed to safeguard VPN users' connections from known malware, Minerva's Anti-Evasion Platform focuses on preventing infections from evasive threats, which are designed to bypass other security tools. Both solutions can be deployed side-by-side to strengthen security posture of remote systems during the VPN session without interfering with users' normal activities.

Unique Benefits of Minerva's Solution

When allowing users to connect to its network over a VPN, enterprises often struggle balancing the need to protect their resources from infected remote systems with imposing strict security requirements on those endpoints. In many cases, the connection is initiated from an unmanaged system—an endpoint that the enterprise doesn't own, for instance when employees use their personal system or when contractors establish the VPN connection from a computer not owned by the enterprise.
Though the organization could impose some security requirements on the connecting system, it often lacks the ability to enforce them or to mandate that the full corporate endpoint security stack be present on the remote host. Minerva's Remote User Protection offers the following benefits:

- Integrates with the organization's VPN software to launch malware scans and to refuse or terminate the connection when necessary.
- Very light weight, able to operate without slowing down the remote user's system.
- Doesn't conflict with security or other non-malicious software on the remote system.
- Provides safeguards against vast numbers of known malware that would otherwise put the enterprise at risk.
- Can be deployed and managed together with Minerva's Anti-Evasion Platform to protect remote workers and the enterprise from advanced threats.

To learn how Minerva's Remote User Protection can address your VPN users' risks and arrange a demo of the solution, please contact your Minerva representative.

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 unknown threats which evade existing defenses by deceiving the malware and controlling how it perceives its environment. Without relying on signatures, models or behavioral patterns, Minerva's solution deceives the malware and causes it to disarm itself, thwarting it before the need to engage costly security resources.
Headquartered in Petach Tikva, 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.**