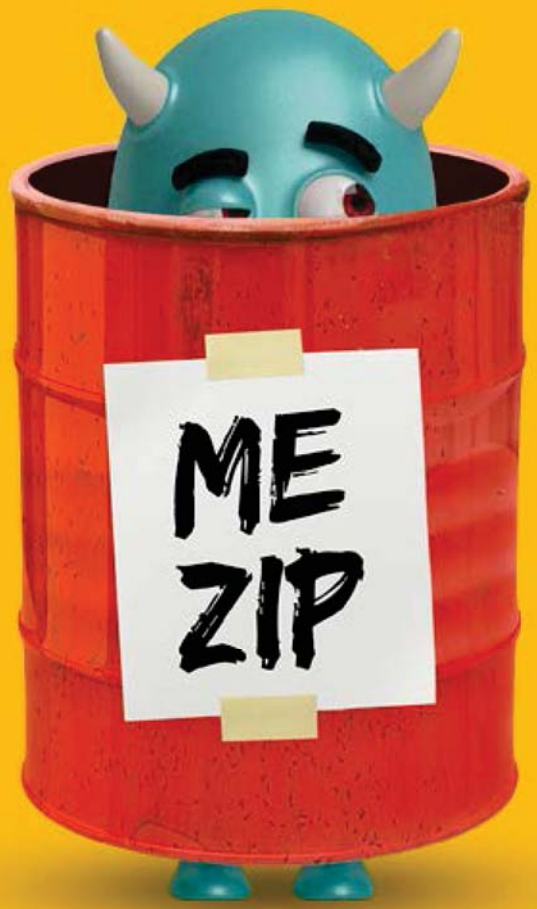
MINERVA

gruppo Daman

Minerva Anti-Evasion Platform

Blocca le minacce sconosciute che sono state progettate per "evadere" i vostri sistemi di sicurezza



La Piattaforma Anti-Evasione Minerva blocca automaticamente gli attacchi che sono stati progettati per superare i vostri sistemi di sicurezza attualmente implementati.

Invece di tentare di rintracciare e identificare i malware, Minerva crea una "realtà virtuale" sulla postazione di lavoro, che induce il malware a mantenersi inoffensivo.

Questo approccio originale, consente all'organizzazione di fermare il potenziale offensivo di malware sconosciuti, evitando di impegnarsi in attività di investigazione o di recovery che risultano molto onerose e poco efficaci.

ATTACCHI SOFISTICATI PROGETTATI PER SUPERARE LE DIFESE ATTUALI

Nonostante gli investimenti in Cyber Security, le postazioni di lavoro vengono ancora infettate da malware. Si tratta di malware avanzati progettati con tecniche evasive, al fine di evitare che gli stessi possano essere identificati dagli strumenti di sicurezza esistenti. Il "codice maligno" contenuto in essi non viene infatti fatto detonare all'interno di Sandbox o in ambienti di analisi forense, ma viene nascosto nella memoria di processi "legittimi" o di documenti, e rimarrà dormiente fino a quando il malware non avrà trovato un ambiente idoneo per attivarlo.

Per combattere queste minacce non è più sufficiente operare in modo tradizionale, tentando cioè di identificare i malware basandosi sui metodi di funzionamento di "codici malevoli" che sono stati identificati in precedenza. Questo modo di operare non è in grado di identificare malware evasivi, sviluppati proprio per evitare di riprodurre metodi implementati in precedenza.

Il risultato di questo scenario è che le organizzazioni spendono le loro energie nell'inseguire e analizzare allarmi che spesso si rilevano dei falsi positivi, e non sono invece in grado di bloccare attacchi che usano tecniche di tipo evasivo.

NON ASPETTATE LA VIOLAZIONE, PREVENITELA...

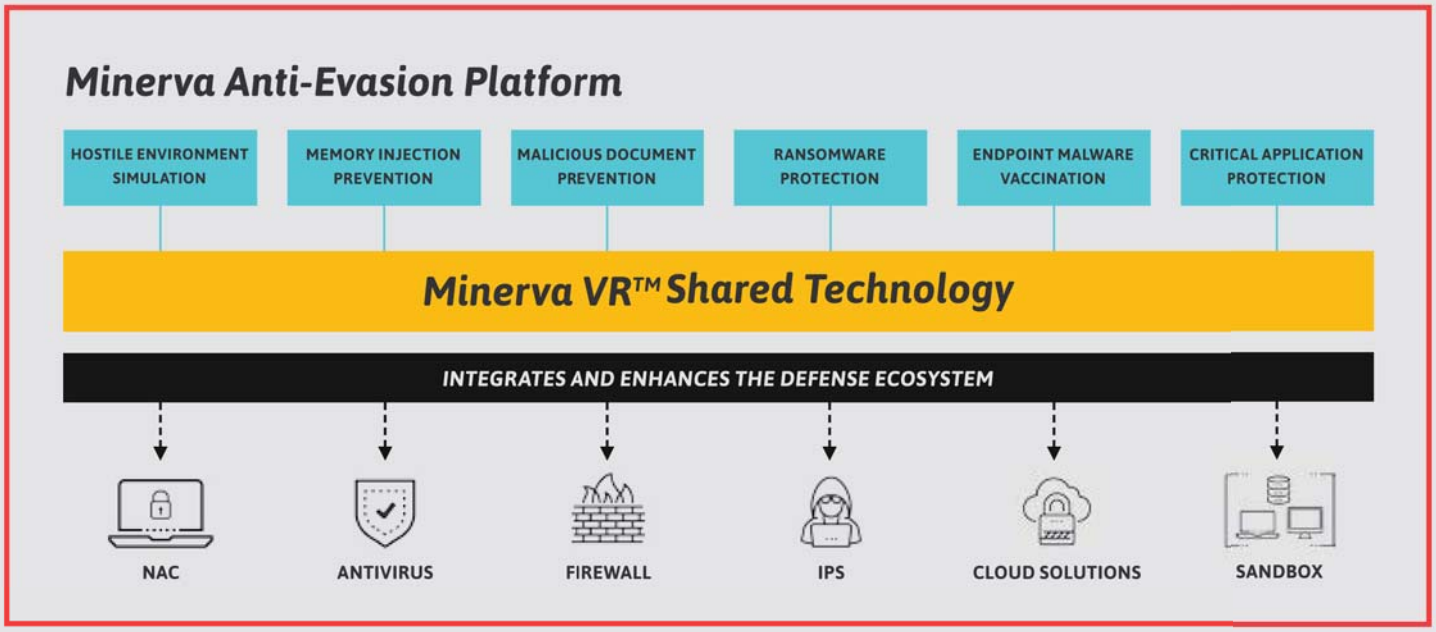
Una volta realizzato che le misure di sicurezza correnti, non sono in grado di offrire una protezione completa delle postazioni di lavoro, le organizzazioni devono pensare a come rafforzare questo sistema di sicurezza. Nella maggior parte dei casi si tratta però di soluzioni che a fronte di malware sconosciuti e che usano tecniche evasive intervengono dopo l'avvenuta violazione, un approccio certamente poco efficace ed efficiente.

CREATE UN AMBIENTE DOVE IL MALWARE SI AUTO DISARMA!

Minerva è focalizzato nella prevenzione di minacce sconosciute, che sono state progettate con tecniche evasive, allo scopo di superare le difese attuali, senza tentare di rintracciare ed identificare questo tipo di malware.

Questo approccio originale nel bloccare attacchi che hanno queste caratteristiche, evita ogni forma di sovrapposizione con altre soluzioni già esistenti, rafforzando il meccanismo di Cyber Defence, indirizzando i punti di debolezza dei metodi basati sull'identificazione del codice maligno.

La Piattaforma Minerva Anti-Evasion (Minerva VR™) agisce sulla "percezione" che il malware ha della postazione di lavoro, realizzando un inganno con il quale disinnesca la minaccia in un modo assolutamente originale e unico sul mercato.



La Piattaforma Minerva rafforza la sicurezza della postazione di lavoro utilizzando un approccio modulare adattabile alle esigenze dell'organizzazione.

Hostile Environment Simulation - usa l'inganno per mantenere dormiente il malware evasivo: risponde infatti alle sue query, quelle con cui il malware cerca di capire se si trova in un ambiente idoneo, simulando un ambiente ostile.

Memory Injection Prevention - blocca i tentativi operati da "fileless malware" o comunque da malware che si nascondono all'interno di processi "legittimi", rendendo queste tecniche inoffensive.

Malicious Document Prevention - blocca attacchi che originano da documenti che contengono macro, PowerShell o altri script. In questo modo Minerva consente di utilizzare le capacità dei moderni documenti, evitando i rischi di sicurezza associati.

Ransomware Protection - intercetta i tentativi dei malware distruttivi di criptare o cancellare documenti ed effettua un backup immediato dei file a rischio.

Endpoint Malware Vaccination - sfrutta un tipico meccanismo implementato dai malware che consiste nel lasciare alcune tracce del proprio passaggio per evitare di infettare lo stesso sistema più di una volta. Minerva diffonde questi "marker" nelle postazioni di lavoro evitando quindi l'infezione da parte del malware.

Critical Application Protection - blocca l'interferenza dei malware con le applicazioni critiche del cliente, nascondendo la presenza di queste applicazioni e dei loro artefatti. In questo modo il malware non sarà in grado di identificare e danneggiare quello che si presenta come un suo target naturale.

KEY BENEFITS

Blocca attacchi sconosciuti ed evasivi
previene attacchi che superano le normali difese con un approccio originale ed efficace

Basso impatto gestionale
rapida implementazione, evitando onerosi processi di rilascio e manutenzione

Nessun impatto sugli utenti
rafforza la sicurezza senza rallentare le operazioni dell'utente finale

Evitare costi di sostituzione
rafforza la sicurezza senza i rischi e i costi di un progetto di sostituzione

FINALMENTE UNA SOLUZIONE DI SICUREZZA CHE NON RENDE PIU' ONEROSE LE ATTIVITA' OPERATIVE

Per garantire un basso impatto operativo, la Piattaforma Minerva Anti-Evasion è una soluzione passiva che non effettua azioni che potrebbero drenare risorse dal sistema, causare falsi allarmi o interferire con applicazioni legittime.

Anche la distribuzione è rapida è a basso impatto, lasciando un'impronta minima e non richiedendo riavvii o complessi prerequisiti.

La piattaforma Minerva Anti-Evasion elimina anche il problema del sovraccarico dovuto alla gestione degli allarmi, evitando la perdita di tempo legata alla gestione dei falsi positivi.

RILASCIO SEMPLICE

Un agente super-thin che può essere installato su migliaia di postazioni in un tempo brevissimo e senza la necessità di ravviare.

OFFLINE MODE

Minerva non richiede continui aggiornamenti e mantiene la sua efficacia anche quando la postazione è fuori della rete.

PREVENZIONE

Minerva evita il carico di lavoro indotto dalle attività di recovery, intervenendo prima che il malware si attivi e provochi danni.

NO FALSI POSITIVI

Ogni allarme prodotto da Minerva corrisponde a una reale minaccia che è stata neutralizzata prima che potesse provocare danni.

BASSO IMPATTO

Minerva non installa agenti pesanti e non esegue scansioni, e quindi non ha significativi impatti sulle performance della postazione.

NESSUNA MANUTENZIONE

Minerva non richiede attività di manutenzione per operare al meglio. Eventuali attività di aggiornamento necessarie a rilasciare nuove funzionalità vengono effettuate senza intervento umano.

gruppo Daman

Minerva è distribuito in Italia dal Gruppo Daman - www.daman.it - info@daman.it - 06.5159281