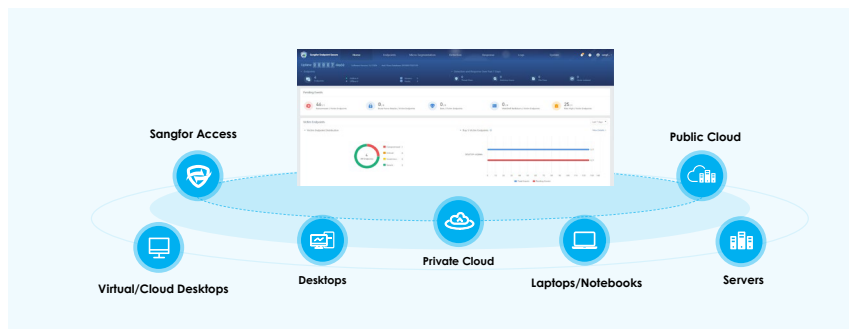


SANGFOR ENDPOINT SECURE

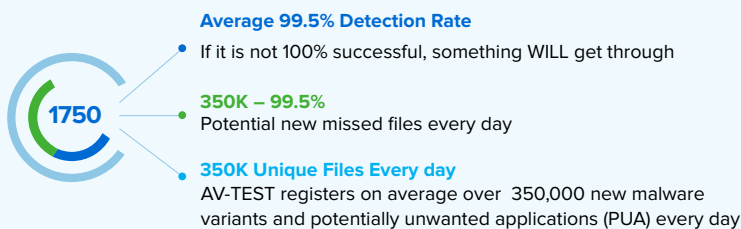
Il futuro della sicurezza degli Endpoint

Sangfor Endpoint Secure rappresenta un diverso approccio alla difesa dei sistemi informatici da malware e advanced persistent threats (APTs).

Endpoint Secure fa parte del framework di sicurezza XDDR di Sangfor, una soluzione veramente integrata, che fornisce una risposta olistica, di facile gestione e manutenzione, alle infezioni da malware e alle violazioni APT che possono colpire l'intera rete aziendale.



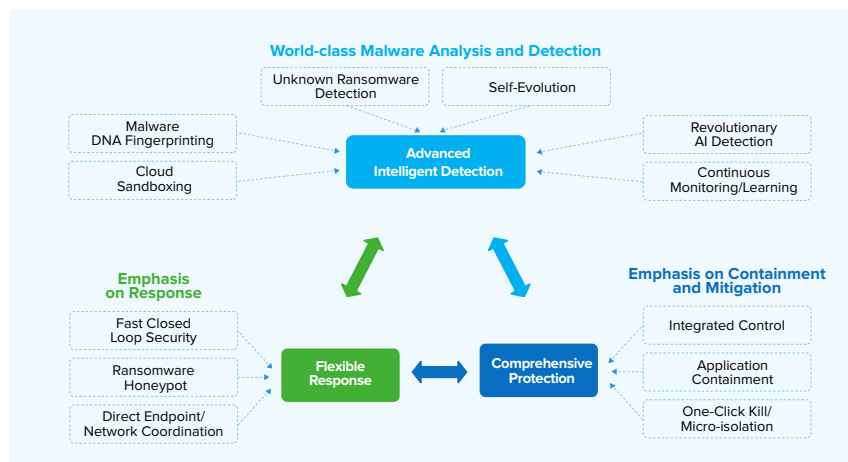
IL DECLINO DEGLI ANTIVIRUS TRADIZIONALI E DI NUOVA GENERAZIONE



Con i prodotti antivirus e anti-malware abbiamo sempre pensato di poter scoprire e bloccare tutti i malware noti e sconosciuti. A tal proposito i test dimostrano che questi prodotti hanno un successo medio del 99,5%.

È quindi evidente che qualcosa riesce ad introdursi nei sistemi, ad esempio, Ransomware si è dimostrato altamente adattabile e di successo, anche di fronte a NGAV distribuito ed a organizzazioni vigili ed attente a questo tipo di attacchi.

UN APPROCCIO DIFFERENTE



Endpoint Secure è un approccio diverso alla protezione degli Endpoint. Anche Engine Zero anti-malware di Sangfor, dotato di motori ad alto tasso di successo di rilevamento, non è efficace al 100%. Nessuna soluzione lo è. Quindi, consideriamo gli anti-malware come "Best Effort". La sicurezza efficace è preparata per "quando" qualcosa passa, non "se" passa.

Basta solo una violazione

Endpoint Secure si concentra sulla risposta, pronta a contenere e mitigare tale violazione, QUANDO questa avviene.

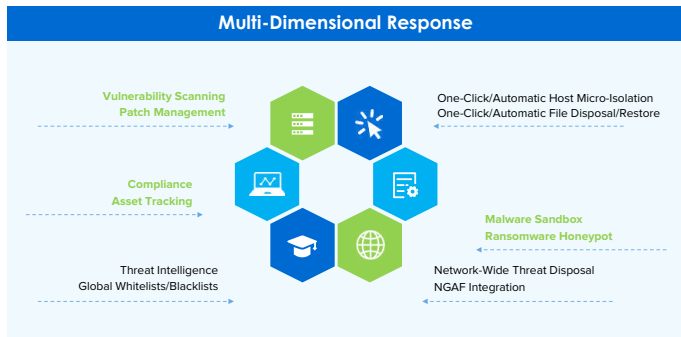




RISPOSTA MULTIDIMENSIONALE

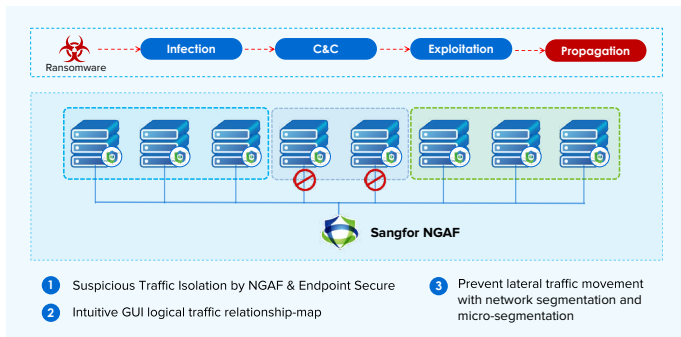
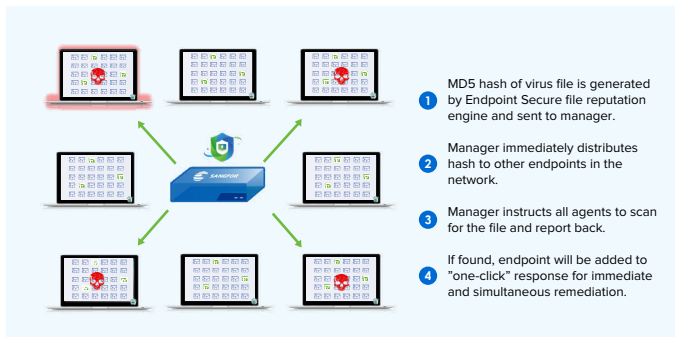
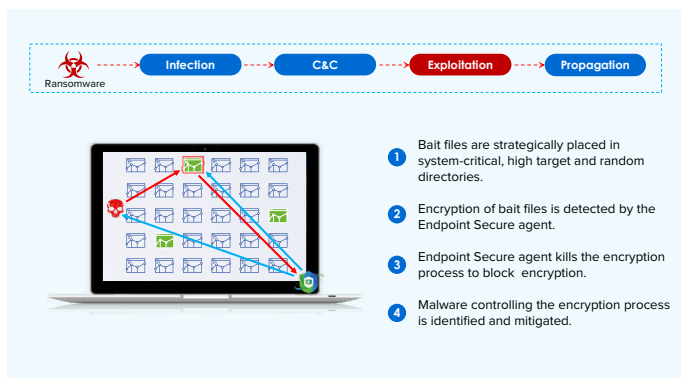
Monitoraggio più semplice ed intelligente

- Scansione delle vulnerabilità pianificata o su richiesta (la scansione può essere avviata dai Firewall Sangfor)
- I risultati della scansione delle vulnerabilità forniscono informative patch recommendation, includendo la global threat correlation.
- Il Compliance Monitoring confronta le endpoint security configuration con le policies di sicurezza dell'organizzazione
- Monitoraggio degli asset aziendali
- Cloud malware sandbox per l'analisi dinamica dei malware
- Funzionalità Endpoint Secure Protect Agent Ransomware Honeypot

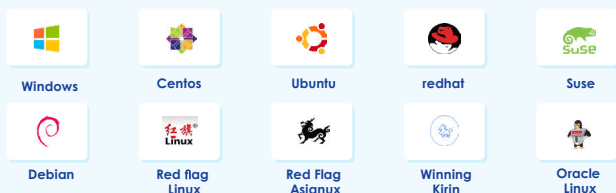


Risposta alle minacce più semplice e intelligente

- Real-time Threat Intelligence da cloud-based Neural-X riconosce nuove firme malware scoperte da Sangfor TI
- One-Click/Automatic Host Micro-Isolation disconnette più endpoint dalla rete, contenendo la diffusione dei malware
- One-Click/Automatic File Disposal elimina o mette in quarantena il malware da più endpoint
- Eliminazione delle minacce a livello di rete consente all'amministratore di rispondere rapidamente a un'epidemia di malware di grandi dimensioni
- L'integrazione con Sangfor NGAF può impedire ai malware di comunicare con i server di "command & control" e quindi di propagarsi all'interno dell'azienda



Operating Systems



Virtualization



Agent

- Less than 200MB memory
- Less than 150 MB disk
- Co-exists with other NGAF

Manager

- 64-bit Ubuntu or CentOS
- CPU: 4 cores
- Memory: min 8GB RAM
- Disk: min 500GB
- HCI and VMWare support

