SANGFOR

SANGFOR ENDPOINT SECURE

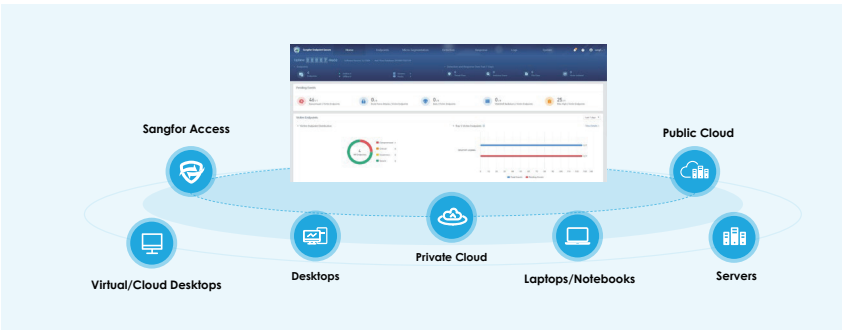
The Future of Endpoint Security

Certification of the Best Windows Antivirus Solution and "TOP PRODUCT" Award by AV-Test

Recommended Windows Protection by Microsoft

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

Average 99.5% Detection Rate
If it is not 100% successful, something WILL get through

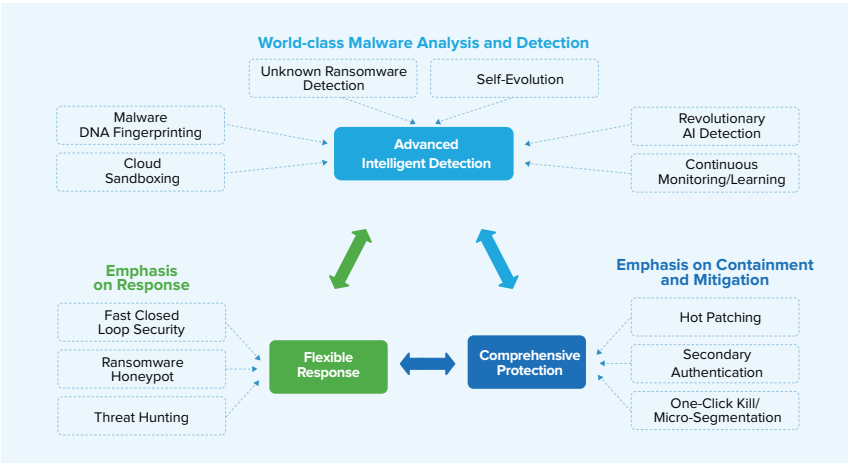
450K * 99.5% = 2250
Potential new missed files every day

450K Unique Files Every day
AV-TEST registers on average over 450,000 new malware variants and potentially unwanted applications (PUA) every day

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.

Contact Us To Know More

Sangfor Technologies sales@sangfor.com marketing@sangfor.com

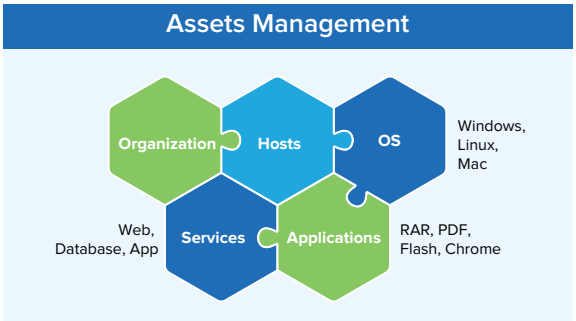
SANGFOR | The Future of Endpoint Security

SICUREZZA DEGLI ENDPOINT A CIRCUITO CHIUSO

❶ Prima di un attacco: prevenire è meglio che curare

Rilevamento e identificazione degli asset degli endpoint

Sangfor Endpoint Secure Manager rileva e identifica automaticamente altri endpoint nello stesso segmento di rete e li raggruppa in base all'organizzazione, agli host, al sistema operativo, ai servizi e alle applicazioni.



Gestione delle vulnerabilità e delle patch

Sangfor Endpoint Secure fornisce sia patch tradizionali che hot patching per le vulnerabilità, garantendo un servizio non-stop e EOS OS.

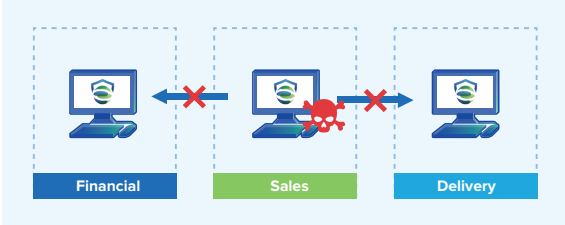
Controllo della linea di base di sicurezza

Sangfor Endpoint Secure supporta i controlli di base di sicurezza basati sulle best practices.

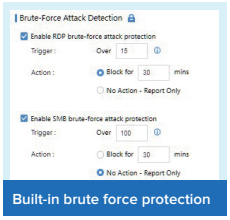
❷ Durante un attacco: non permettere alle minacce di nascondersi

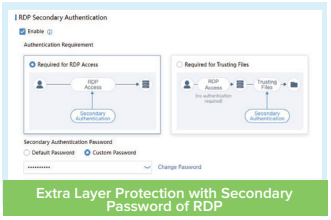
Capacità di rilevamento delle minacce leader a livello mondiale

Sangfor Endpoint Secure utilizza una combinazione di rilevamento basato sulla firma, rilevamento avanzato del malware tramite AI, intelligence delle minacce in tempo reale, e cloud sandboxing per identificare il comportamento anomalo sugli endpoint.



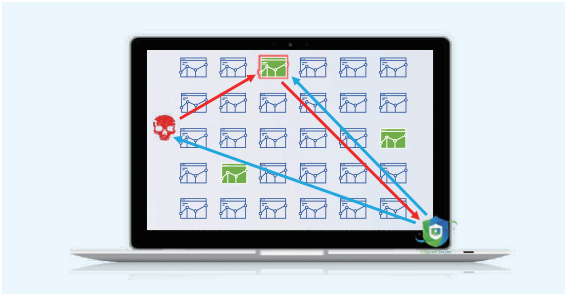
Ciò consente a Endpoint Secure di rilevare sia gli exploit zero-day sconosciuti sia i più sofisticati attacchi informatici con velocità e precisione. Si è guadagnato il riconoscimento di "TOP PRODUCT" nell'AV-Test per tre anni consecutivi.





Enpoint a basso impatto

Sangfor Endpoint Secure offre un'eccezionale capacità di rilevamento consumando risorse di sistema minime per offrire un'esperienza utente fluida. Nei test condotti da AT-Test, Endpoint Secure ha ottenuto il più basso impatto complessivo sulla velocità delle operazioni quotidiane dei PC aziendali.



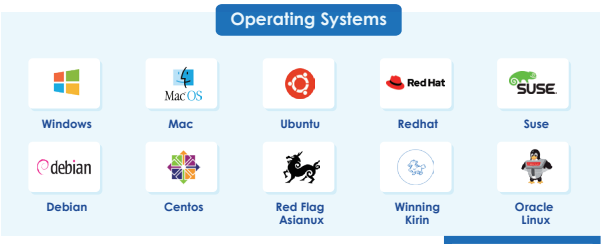
Caratteristiche di sicurezza innovative

Sangfor Endpoint Secure è integrato con molte caratteristiche innovative che rilevano e rispondono a una varietà di minacce. Il rilevamento di attacchi con "forza bruta" e l'autenticazione a due fattori proteggono i sistemi da accessi non autorizzati. L'isolamento dell'host compromesso impedisce alle minacce di spostarsi lateralmente da un host all'altro. Il primo e unico endpoint ransomware honeypot al mondo rileva e uccide attacchi ransomware in tempo reale.

❸ Dopo un attacco: Controlla le lacune della sicurezza per prevenire danni futuri

Eliminare le minacce residue attraverso la caccia alle minacce

Sangfor Endpoint Secure è dotato di una funzione di Threat Hunting che rileva ed elimina eventuali minacce residue nell'intera rete.



Correlazione e integrazione

Sangfor Endpoint Secure supporta la correlazione delle minacce con Sangfor NGAF, IAG, Cyber Command, e altri componenti del sistema Sangfor Extended Detection, Defence, and Response (XDDR).

Contact Us To Know More

Sangfor Technologies sales@sangfor.com marketing@sangfor.com