RASISS

TAKING CARE OF YOUR DIGITAL LIFE

SANGFOR | Endpoint Secure

Endpoint Secure

Endpoint Security

The Future of Endpoint Security

Website: www.rasiss.com

Email: Info@rasiss.com

Phone: 051-38478130-35

مقدمه:

شرکت سنگفور (Sangfor)یک ارائه‌دهنده پیشرو در زمینه راهکارهای امنیت سایبری، شبکه و زیرساخت‌های IT است که از سال 2000 فعالیت خود را آغاز کرده و به دلیل تخصص خود در امنیت اطلاعات، بهبود شبکه‌های سازمانی و ایجاد زیرساخت‌های دیجیتالی امن، شهرتی جهانی کسب کرده است. سنگفور با تمرکز بر توسعه محصولات نوآورانه و به‌روز در حوزه‌های مختلف مانند فایروال‌های نسل جدید(NGFW) ، امنیت نقاط انتهایی (Endpoint Security)، دسترسی ایمن به شبکه(SASE) و مدیریت تهدیدات پیشرفته، به سازمان‌ها کمک می‌کند تا در برابر حملات سایبری پیچیده و تهدیدات نوظهور محافظت شوند. این شرکت با استفاده از فناوری‌های پیشرفته مانند هوش مصنوعی و یادگیری عمیق، تلاش دارد راهکارهای جامعی برای مقابله با چالش‌های امنیتی مدرن ارائه دهد.

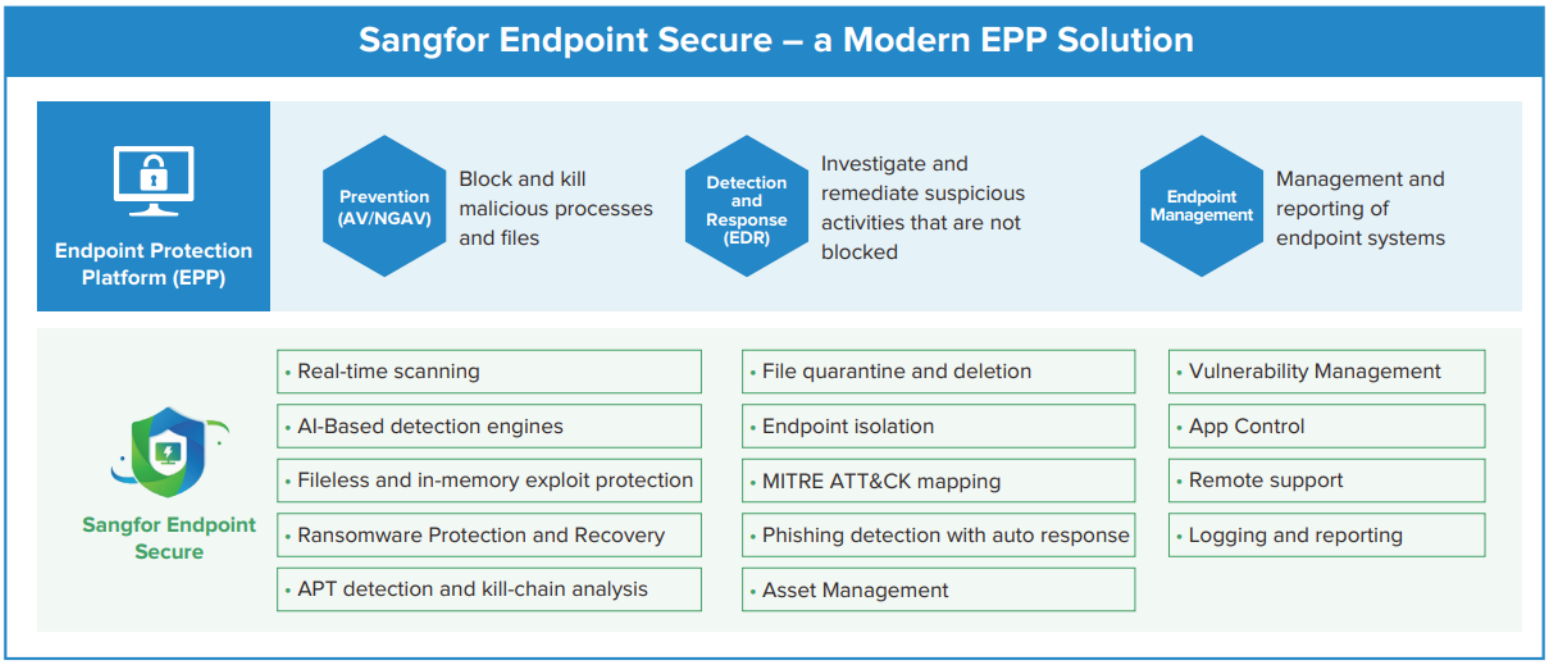
Sangfor Endpoint Secure:

Sangfor Endpoint Secureیکی از محصولات برجسته سنگفور برای حفاظت از نقاط انتهایی سازمان است که با تکیه بر تکنولوژی‌های پیشرفته‌ای مانند هوش مصنوعی (AI) و یادگیری ماشین، از کامپیوترها و دستگاه‌های کاربران نهایی در برابر تهدیدات مختلف محافظت می‌کند. این محصول نه تنها بدافزارها و حملات شناخته‌شده را شناسایی می‌کند، بلکه توانایی مقابله با تهدیدات پیچیده و ناشناخته، مانند باج‌افزارها و حملات بدون فایل (fileless attacks) را نیز داراست Endpoint Secure .با ترکیب قابلیت‌های پیشرفته در زمینه شناسایی، پیشگیری، و واکنش به تهدیدات، یک راه‌حل جامع برای امنیت نقاط انتهایی در محیط‌های سازمانی فراهم می‌کند.

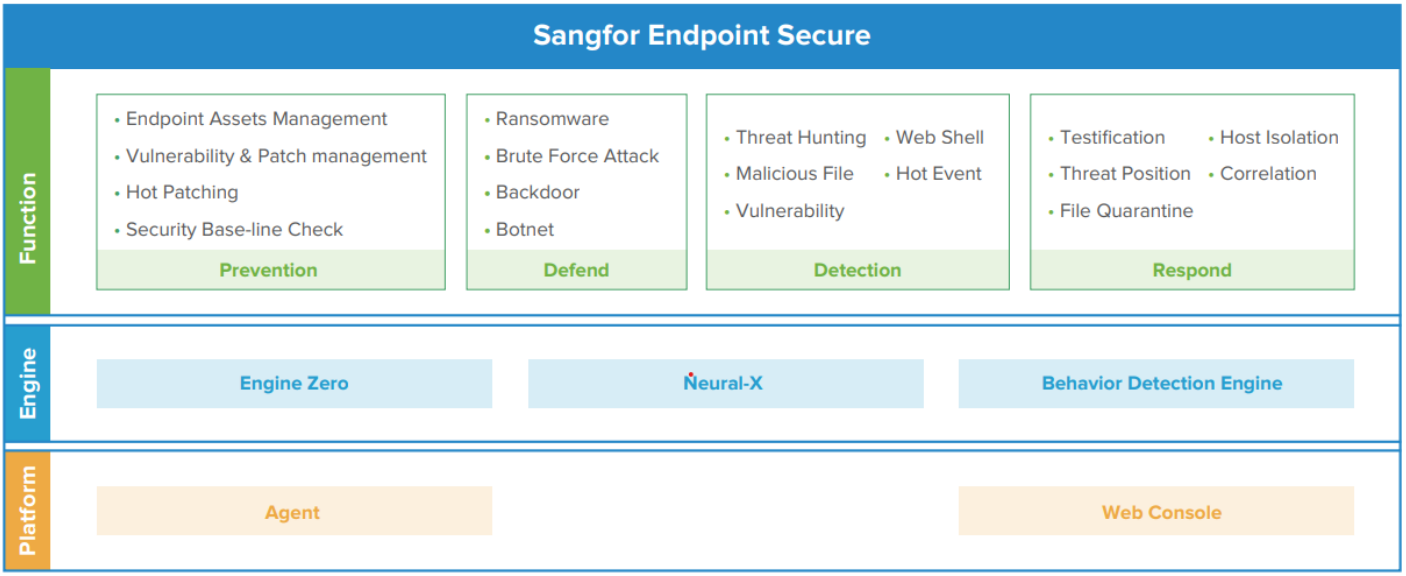
قابلیت‌های ردیابی و واکنش سریع یکی از نقاط قوت مهم این محصول است. این قابلیت‌ها به سازمان‌ها کمک می‌کند تا بتوانند تمامی فعالیت‌های مشکوک را ردیابی کرده و منبع تهدیدات را به سرعت شناسایی کنند. به‌علاوه، Endpoint Secure می‌تواند از زنجیره حملات استفاده‌شده توسط مهاجمان آگاه شود و با جلوگیری از انتشار ویروس یا بدافزار به سایر نقاط شبکه، مانع از گسترش تهدیدات شود.

از دیگر ویژگی‌های مهم Sangfor Endpoint Secure می‌توان به حفاظت پیشرفته از باج‌افزارها و بازیابی اطلاعات اشاره کرد. این محصول با مانیتورینگ لحظه‌ای فرآیندهای مشکوک، فعالیت‌های مرتبط با باج‌افزارها را شناسایی و مسدود کرده و از رمزگذاری فایل‌های کاربران جلوگیری می‌کند. در صورت رمزگذاری فایل‌ها، قابلیت بازیابی خودکار از طریق سرویس پشتیبان (مانند Windows VSS) فراهم است، که به سازمان‌ها امکان می‌دهد تا اطلاعات خود را به حالت اولیه بازگردانند.

با استفاده از Endpoint Secure، سازمان‌ها می‌توانند با اسکن نقاط انتهایی خود برای شناسایی پیکربندی‌های خطرناک و آسیب‌پذیری‌ها، اقدامات پیشگیرانه‌ای را انجام دهند، هنگام وقوع تهدیدهای امنیتی تحقیقاتی را صورت دهند و با راهکاری آسان و کارآمد، به سرعت واکنش نشان دهند. قابلیت‌های مدیریت نقاط انتهایی در Endpoint Secure شامل مدیریت آسیب‌پذیری‌ها و پچ است که به کاهش ریسک‌ها و بهبود انطباق کمک می‌کند. مدیریت سیاست‌های متمرکز و عیب‌یابی از راه دور نیز به تیم‌های عملیاتی کمک می‌کند تا فرآیند عملیات و نگهداری (O&M) را ساده و کارآمدتر کنند.



معماری Sangfor Endpoint Secure:



1. **Platform (پلتفرم)**

- **Agent:** این بخش در واقع عامل نصب‌شده بر روی دستگاه‌های انتهایی است که داده‌ها را جمع‌آوری و اقدامات لازم را اجرا می‌کند.
- **Web Console:** کنسول وب به مدیران اجازه می‌دهد به‌طور متمرکز سیاست‌ها را مدیریت کنند، تهدیدات را مانیتور کنند و گزارش‌ها و لاگ‌های امنیتی را مشاهده کنند.

2. موتورهای تشخیص تحلیل (Engine)

- **Engine Zero:** این موتور، تحلیل اولیه و پایه‌ای را انجام می‌دهد و احتمالاً به تشخیص سریع تهدیدات شناخته‌شده و مدیریت پایه‌ای تهدیدات می‌پردازد.

- **Neural-X:** یک موتور تحلیل مبتنی بر هوش مصنوعی و یادگیری ماشین که تهدیدات پیچیده‌تر و ناشناخته را شناسایی می‌کند و می‌تواند رفتارهای غیرعادی را تشخیص دهد.
- **Behavior Detection Engine:** این موتور به‌طور خاص روی تحلیل رفتار تمرکز دارد و رفتارهای مشکوک را برای تشخیص تهدیدات بررسی می‌کند، که به‌ویژه در برابر تهدیدات بدون فایل و حملات پیچیده کاربردی است.

3. Function (کارکرد)

این بخش شامل مجموعه‌ای از کارکردهای مختلف برای مدیریت امنیت دستگاه‌های انتهایی است:

- **Prevention (پیشگیری)**
  - **Endpoint Assets Management**: مدیریت دارایی‌های نقطه انتهایی و دستگاه‌ها.
  - **Vulnerability & Patch Management**: مدیریت آسیب‌پذیری‌ها و پچ‌های امنیتی.
  - **Hot Patching:** اعمال سریع پچ‌ها بدون نیاز به ریبوت یا توقف سرویس.
  - **Security Baseline Check**: بررسی سطح پایه‌ای امنیت برای اطمینان از رعایت استانداردهای امنیتی.
- **Defend (دفاع):**
  - **Ransomware:** مقابله با تهدیدات باج‌افزاری.
  - **Brute Force Attack**: شناسایی و جلوگیری از حملات بروت فورس.
  - **Backdoor**: شناسایی و مسدودسازی درب‌های پشتی (backdoors) که ممکن است در سیستم ایجاد شده باشند.
  - **Botnet**: تشخیص و جلوگیری از آلوده‌شدن به بات‌نت‌ها.
- **Detection (شناسایی)**
  - **Threat Hunting**: شکار تهدیدات و شناسایی فعالیت‌های مشکوک.
  - **Malicious File**: شناسایی فایل‌های مخرب.
  - **Vulnerability**: شناسایی آسیب‌پذیری‌های موجود در دستگاه‌ها.
  - **Web Shell & Hot Event**: شناسایی فعالیت‌های غیرمجاز مبتنی بر شل و رویدادهای امنیتی مهم.
- **Respond (پاسخ)**

Testification: ارائه گواهی برای بررسی و تجزیه و تحلیل تهدیدات.

  - **Host Isolation**: ایزوله کردن دستگاه آلوده برای جلوگیری از گسترش تهدید.
  - **Threat Position**: موقعیت‌یابی تهدید در شبکه برای تسهیل شناسایی و حذف آن.
  - **File Quarantine**: قرنطینه کردن فایل‌های مشکوک برای جلوگیری از اجرای آنها.
  - **Correlation**: همبستگی بین رویدادهای امنیتی مختلف برای درک بهتر زنجیره حملات و یافتن منبع آن.

به صورت کلی این معماری با بهره‌گیری از موتورهای تشخیص مختلف، یک ساختار چندلایه‌ای را ارائه می‌دهد که به شناسایی، پیشگیری، دفاع و پاسخ‌دهی به تهدیدات امنیتی در نقاط انتهایی کمک می‌کند.

مقایسه نسخه های مختلف Sangfor Endpoint Secure:

Feature/Module	Ultimate	Essential
Vulnerability Scan	✓	✓
Remediation	✓	✓
Security Compliance Check[1]	✓	✓
Asset Inventory	✓	✓
Asset Discovery	✓	✓
TOTP Authentication[2]	✓	✓
Realtime File Monitoring	✓	✓
Ransomware Honeypot	✓	✓
Ransomware Protection	✓	✓
Ransomware Backup Recovery	✓	✓
Ransomware Defense	✓	✓
End-of-Support Windows System Protection	✓	✓
Malicious File Detection	✓	✓
Botnet Detection	✓	✓
Brute-Force Attack Protection	✓	✓
Improved Phishing and Web Intrusion Detection	✓	✓
Suspicious Login Detection	✓	✓
File Quarantine	✓	✓
Endpoint Isolation	✓	✓
File Remediation	✓	✓
Virus Mitigation	✓	✓
Automated Response to Phishing and Web Intrusion events	✓	✓
Domain Isolation	✓	✓
Process Blocking	✓	✓
Script File Upload	✓	✓
USB Control	✓	✓
Unauthorized Outbound Access Detection	✓	✓
Remote Support	✓	✓
Hot Patching [3]	✓	✗
Endpoint Behavior Data & Log Collection	✓	✗
Fileless Attack Protection	✓	✗

Feature/Module	Ultimate	Essential
RDP Secondary Authentication (Anti-Ransomware)	⚑	⚑
Trusted Processes (Anti-Ransomware)	⚑	⚑
Key Directory Protection (Anti-Ransomware)	⚑	⚑
Coordinated Malware Response with XDDR	⚑	⚑
WebShell Detection	⚑	⚑
Advanced Threat Detection	⚑	⚑
Memory Backdoor Detection	⚑	⚑
Reverse Shell Detection	⚑	⚑
Local Privilege Escalation Detection	⚑	⚑
Remote Command Execution Detection	⚑	⚑
Extended Detection, Defense and Response (XDDR)	⚑	⚑
Threat Hunting	⚑	⚑
Application Blacklist	⚑	⚑
Software Metering	⚑	⚑
Software Uninstallation	⚑	⚑

[1] بررسی وضعیت امنیتی دستگاه (ازجهت فعال بودن فایروال و به روزرسانی سیستم عامل) و همچنین انطباق با استانداردهای امنیتی (مانند سطح پیچیدگی رمزعبور، عدم وجود نرم افزارهای مخرب) و در نهایت ارائه گزارشات در این زمینه

[2] احراز هویت مبتنی بر کد یکبار مصرف زمان‌دار یا Time-Based One-Time Password، با تولید یک کد یکبار مصرف که تنها برای مدت کوتاهی (معمولاً ۳۰ یا ۶۰ ثانیه) معتبر است، امنیت ورود به سیستم را ارتقا می‌دهد.

[3] به فرآیند اعمال تغییرات و اصلاحات در نرم‌افزار یا سیستم‌ها بدون نیاز به توقف یا راه‌اندازی مجدد آنها اطلاق می‌شود.

راه های ارتباطی جهت کسب اطلاعات بیشتر:

تلفن: 5-38478130-051 داخلی: 3

ایمیل: info@rasiss.com