SANDFOR ENDPOINT PROTECTION AND RESPONSE PLATFORM

Endpoint Secure

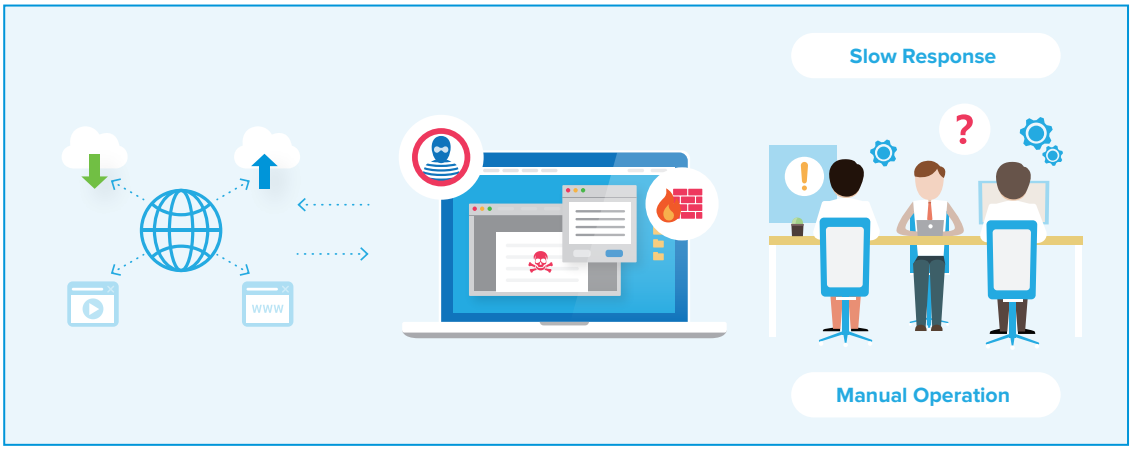
SANGFOR

Enterprise-level endpoints face serious security challenges in a new era

Enterprise LAN endpoints and data have significant value to cyber criminals, putting endpoints, servers, software and hardware at serious risk of attack from complex and sophisticated viruses, ransomware and various other propagation modes. These serious endpoint security challenges as well as increasingly strict regulations on protection, management and applications make proactive endpoint protection critical.

Manual operation and maintenance increases the cost of defense

Traditional endpoint security products operate on common policies and characteristics, often based on more traditional organizational rules and operation regulations, designed to defend against threats from known sources. Organizations utilizing this more traditional approach to security, yet suffering attack from more complex and advanced threats, often experience an exponential increase in labor costs, while specialized enterprise O&M personnel have inadequate experience to effectively respond to the threat.

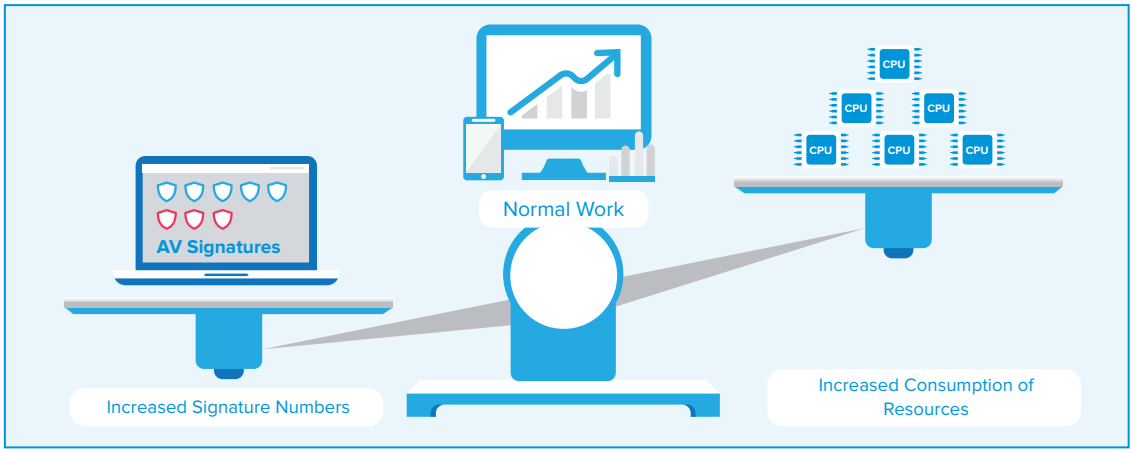


Feature matching response to viruses is inadequate protection to new attack methods

In environments where there is constant risk from advanced threat, virus prevention methods utilizing the more passive antivirus database identification and response methods are often penetrated by newer viruses and ransomware. In addition, the limited capacity of local feature databases often fails to meet basic protection requirements against unknown and even some known viruses.

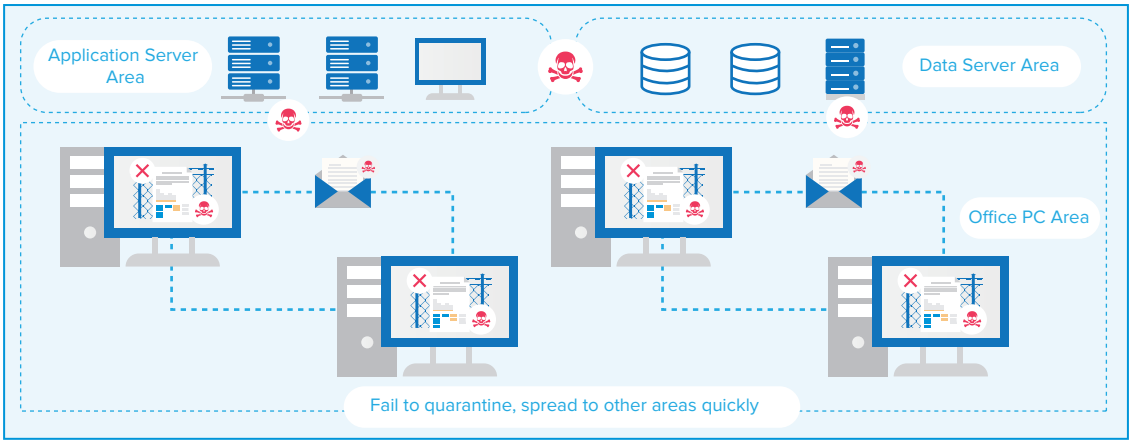
High-capacity antivirus feature databases lead to increased host computing resource costs

The gradual increase in quantity of antivirus feature databases increases the cost of endpoint storage and computing resources. When threat defense monopolizes a significant amout of work hours and employee effort, users are unable to focus on optimization scenarios such as shifting to the cloud.



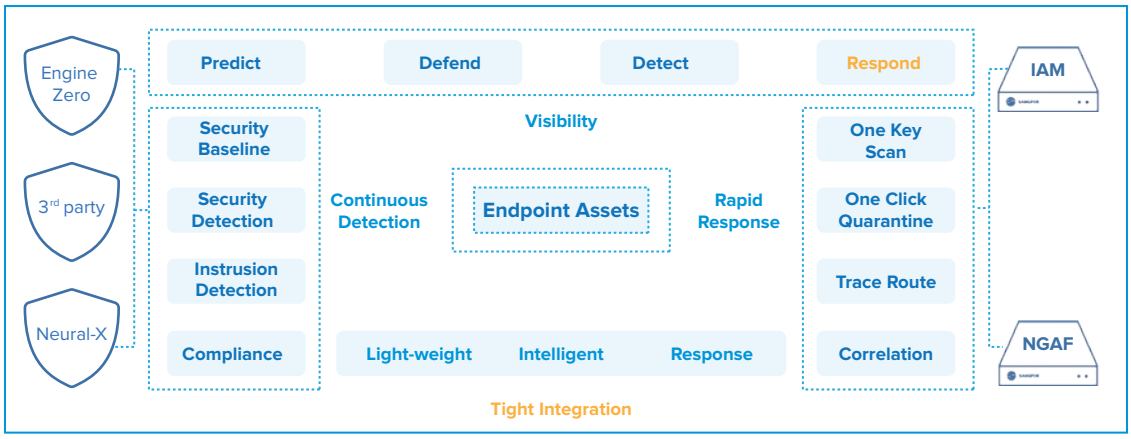
Outdated virus protection is incompatible with new propagation modes and virus environments

Virus killing based on the file isolation method is outdated, with failure allowing a single-point threat to spread quickly. New viruses and propagation modes are often able to bypass traditional antivirus products, which are not designed to adapt to new threats and environments.

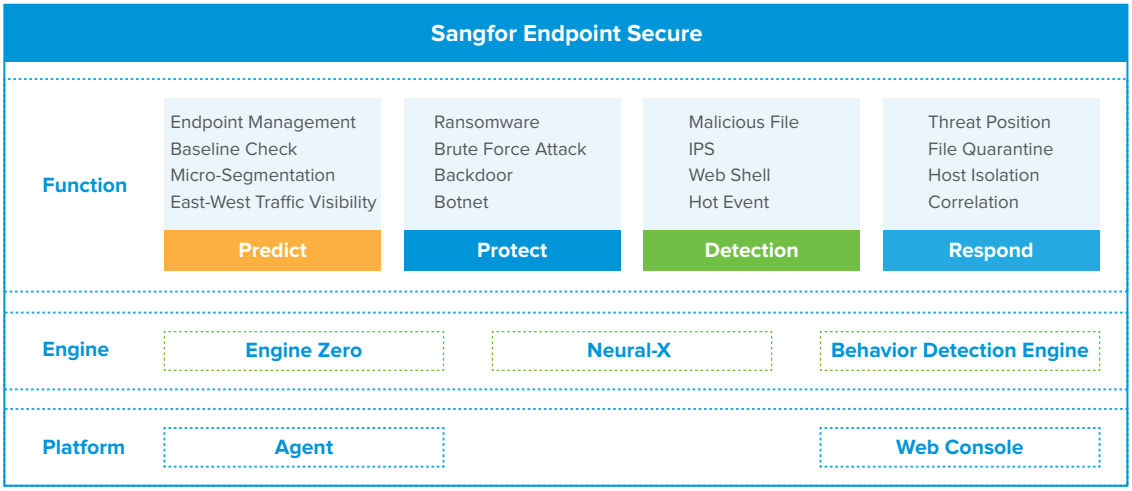


Sangfor Endpoint Protection and Response Platform

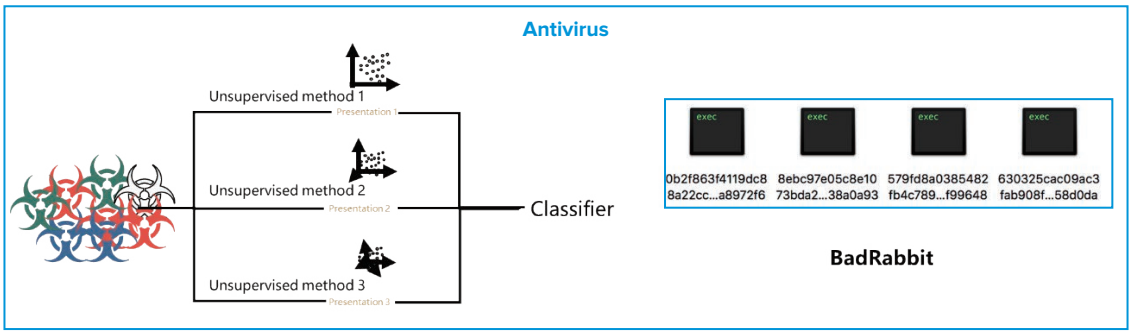
Sangfor's Endpoint Protection and Response platform (Endpoint Secure) provides the endpoint with a more detailed isolation policy, enabling more accurate search and destroy capabilities, sustainable detection capabilities and faster processing capabilities including prevention, defense, detection and response. Endpoint Secure is constructed through cloud linkage and coordination, threat information sharing and multi-level response mechanisms. Advanced threat response is immediate, with Endpoint Secure providing users with assistance dealing with any endpoint security problems by way of its new, light-weight, intelligent and instantaneous endpoint security system.



Architecture of Endpoint Protection and Response Platform



Application Scenarios



Risk Scenario:

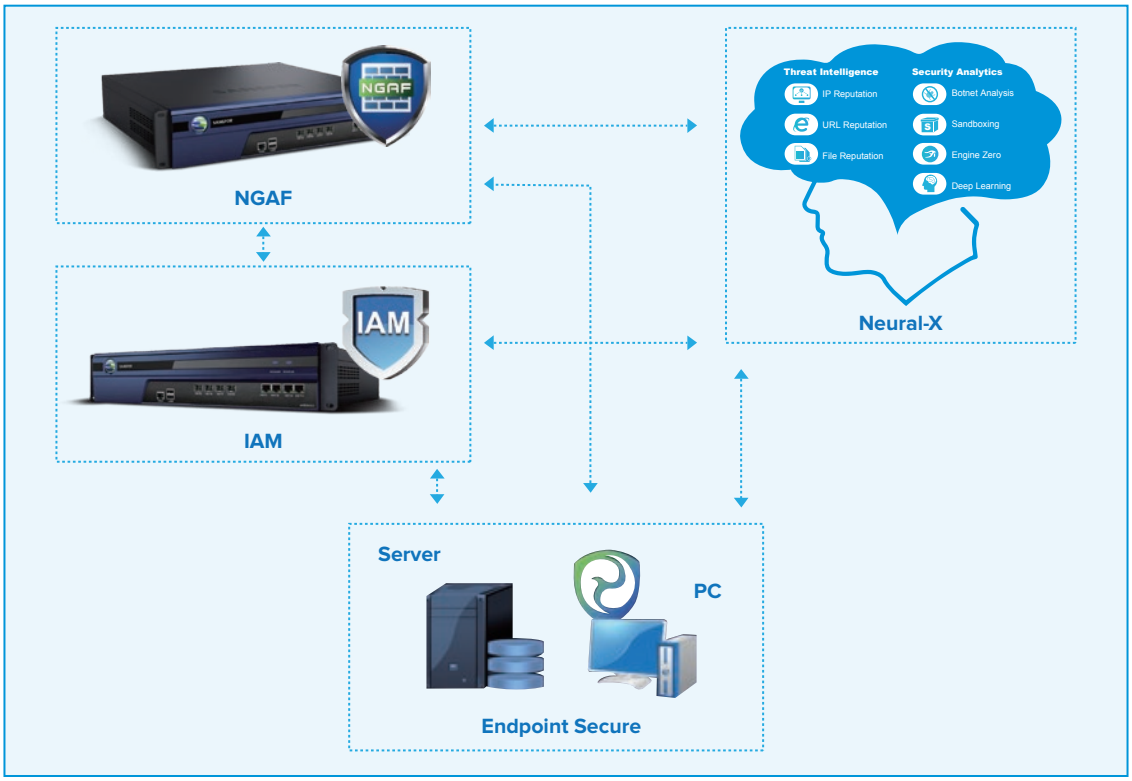
Internal endpoints are characterized by widespread coverage, numerous points and office networks. Attacks from unknown viruses or ransomware significantly affect business critical applications, compromising the security of core internal data.

1. The lack of resources available to detect and respond to advanced and unknown threat prevents proactive defense.
2. Manual system management is inadequate when dealing with fast-moving and unknown threat – exposing the system

Endpoint Secure Application Effects:

1. An AI core and the supplementation of the reputation database, gene and behavior analysis functions provides a 100% threat defense system capable of immediate and comprehensive detection and prevention.
2. Multi-dimensional innovative micro-segmentation technology and intelligent coordination of cloud-pipe-device functions provide immediate identification and response and comprehensive threat neutralization.

Device Linkage



Risk Scenario:

While most internal infrastructure utilizes firewall, intrusion prevention and other various border gateway devices, many gateway devices perform their own independent functions, preventing cohesive and effective security defense.

1. Gateway devices acting independently to prevent malicious attack means that once the boundary is breached, the malicious attacker propagates rapidly and can't be controlled.
2. Even if the external threat is known, effective shared linkage with the endpoint cannot be formed and endpoint control cannot be achieved.

Application Effects:

1. Endpoint Secure can be coordinated and linked with Sangfor Neural-X, AF and AC to form a three-dimensional defense structure covering the cloud, boundary and endpoint, sharing the internal and external threat information in real time.
2. The Endpoint Secure intelligent linkage mechanism shares external threat information in a timely manner, allowing automatic response.

Advantages and Characteristics

New Artificial Intelligent Antivirus Engine

Sangfor Engine Zero

Sangfor Anti-Malware Engine

Artificial Intelligence Based Non-Signature Engine

Detect Unknown Malware Accurately

Unlike traditional antivirus engines, Engine Zero has adopted artificial intelligence (AI) featureless technology, enabling effective identification of unknown viruses and variants, including those unlisted in the antivirus database.

High Compatibility

Windows xp sp3 Windows 7 Windows 8.1 Windows 10 Windows 2003 sp2 Windows 2008 Windows 2008R2 Windows 2012 Windows 2016	CentOs 5 CentOs 6 CentOs 7	Ubuntu 10 Ubuntu 11 Ubuntu 12 Ubuntu 13 Ubuntu 14 Ubuntu 15 Ubuntu 16	redhat 5 redhat 6 redhat 7	Debian 6 Debian 7 Debian 8 Debian 9	SuSE linux 12	Oracle Linux 6	Red Flag Asianux Server 4