Sangfor Endpoint Secure

Competitive Analysis Against Symantec

www.sangfor.com

SANGFOR

Symantec Advantages and Disadvantages

Gartner Summary

Symantec is an industry veteran and continues to be the leading competitive threat mentioned by other vendors in this research. Broadcom, a global semiconductor provider, announced an agreement to acquire the enterprise security business of Symantec on 8 August 2019.

Symantec launched Complete Endpoint Defense that includes Symantec Endpoint Protection 15 (SEP 15) cloud-managed EDR, and attack surface reduction capabilities, all delivered through a single agent. Symantec EDR has the largest EDR market share of the traditional vendors. In 2018, Symantec made a number of acquisitions including Javelin Networks to protect Active Directory, Appthority to provide mobile application testing and catalog of known-good mobile applications, and Luminate Security, which provides secure remote access to data center applications.

Symantec's strategic direction is to provide an Integrated Cyber Defense (ICD) Platform to unite the broader portfolio of security products (including DLP, Web Security Service [WSS] and CASB) with a consolidated agent, data and reporting platform for monitoring and incident response (ICD Manager).

Symantec remains a solid competitor and a good choice for most organizations.

Advantages

01

Symantec has embraced a cloud-first strategy with the introduction of its latest product updates, including SEP 15 and EDR, which provide a cloud-based console with feature parity to the on-premises management console and ability to run hybrid scenario.

02

Complete Endpoint Defense introduces new features such as deception breadcrumbs to improve detection of active attackers, application allow-listing capabilities, vulnerability detection and remediation, and a VPN. SEP 15 also introduced automated posture assessment including vulnerability management and remediation technology.

03

Symantec EDR is a capable EDR tool with extensive APIs for integration and automation with other security and system management tools.

04

Symantec provides a very comprehensive endpoint security solution, Symantec Complete Endpoint Defense (CED), which covers multiple areas to include anti-malware, EDR, app isolation, app control, Active Directory defense and cloud connect defense on PC, Mac, Linux and mobile devices. Symantec also offers vulnerability remediation and endpoint management, mobile security (SEP Mobile), and a managed EDR service.

05

Symantec's broad deployment across a very large deployment population of both consumer and business endpoints provides it with a very wide view into the threat landscape across many verticals.

Cautions

- The acquisition by Broadcom was not factored into this analysis as the acquisition has not closed. The acquisition by Broadcom adds some uncertainty to Symantec's execution. Broadcom's goals may not align with Symantec's customers' aspirations for the Sangfor Endpoint Secure.
- Symantec's has undergone numerous management changes over the past several years, including the recent departure of its CEO and replacement of several key managers. Symantec has been gradually losing market share as the market becomes more competitive, and it has lost its first place in market share by seat licenses to Microsoft.
- Although Symantec has made significant investments in integrating its various products into a more cohesive middleware platform called Symantec Integrated Cyber Defense Exchange(ICDx), it is still lacking a universal incident response environment. However, Symantec does offer a rich set of APIs to integrate with other security tools.
- Symantec EDR is missing advanced functions for large enterprise customers, such as case management workflow, remote shell response function (due 1Q20) and rapid pivot capabilities from one query to another. EDR does not provide blocking rules although automated actions can be scripted for specific detections. The user interface lacks guided investigation tips or contextual information, which makes it difficult to use for mainstream buyers. EDR and SEP are different management consoles.
- SEP 15 Cloud console is relatively new and, although Symantec reports 55% of customers are using cloud, the vast majority are not using SEP 15 Cloud console. SEP Cloud is not FedRAMP certified.

02

Sangfor Endpoint Secure VS Symantec

Competitive Comparison

Features	Symantec	Sangfor
Asset management	Support	Support
Endpoint discovery	Unsupported	Support (Sangfor can view the installation rate, discover endpoints, unconfirmed endpoints, inactive devices and can clearly count managed and unmanaged endpoints.)
Storage control	Support	Support
Intelligent detection engine	Support	Support
Vulnerability patch management	Unsupported (Symantec does not have the vulnerability scanning, vulnerability repair and patch distribution functions of anti-virus software. Instead, it uses the host integrity strategy to check whether the corresponding patch has been applied.)	Support
Email protection	Support	Unsupported
Micro segmentation (firewall)	Support	Support

Features	Symantec	Sangfor
Vulnerability attack protection	Support	Support
Global threat intelligence	Support	Support
Macro virus disposal	Support	Support
Ransomware disposal	Unsupported (Without feature detection, layered technology of key endpoint protection, lateral movement control and decoy technology to fully resist malicious ransomware and unknown attacks. Symantec mainly relies on the main defense capability and does not support ransomware protection, ransomware document catalog protection, ransomware encryption compensation)	Support
Network file search	Unsupported	Support (The entire network can be searched for the specified MD5 file, and the host name, file description, version, HASH value, security level and other information of the searched file can be displayed, and further processing of the file is supported)
Domain name search	Unsupported	Support (The entire network can be searched for the specified domain name, and the host name, process name, process file description, process file version, HASH value and other information that access the domain name can be displayed, and further processing of files is supported)
Firewall-endpoint integration protection	Unsupported	Support
Endpoints remote management	Unsupported (Only supports restarting the endpoints' system)	Support
Policy management	Support (Able to provide strategic adaptation capabilities based on geographic location)	Unsupported
Log report management	Support	Support
Account permissions	Support	Support
Malicious communication interception	Support	Support
USB control	Support	Unsupported (Cooperated with IP-guard)

How to Win Against Symantec —Sangfor Endpoint Secure's Selling Points

Sangfor Endpoint Secure Advantages

01 Endpoint security operation and maintenance functions are relatively complete and easy to use

- Frankly speaking, Symantec SEP may still focus on anti-virus analysis, but it lacks a closed-loop operation and maintenance perspective, such as how to allow administrators to easily see the entire network, how to effectively remotely control endpoints, and how to directly scan and detect risks and vulnerabilities. How to summarize experience and lessons through comprehensive report analysis and improve the overall defense strategy.

02 Advantages of ES at the operation and maintenance level

- Security administrators can use ES to overview the entire network threats, what are the current problems of each endpoint in real time. Symantec SEP does not provide this kind of whole perspective of risk perception and presentation ability, and this kind of ability is very needed by operation and maintenance engineer.
- Sangfor ES micro-segmentation function can be tailored to the isolation strategy of each endpoint/endpoint group/business domain and the flow between endpoints in the network is visible.

03 Closed loop protection and quick response

- At the endpoint security protection level, Sangfor ES has a small closed loop and a large closed loop, forming a complete capability coverage.
- Small closed loop: Sangfor ES forms a small closed loop of endpoint security from prevention-protection-detection-response-operation.
- Large closed loop: the multi-product integration loop, supports integration with NGAF/IAM/CC/security service SOC platform, cloud etc. The large closed loop can make the detection and killing more accurate, and greatly improve the efficiency of threat disposal. It is a great value for security operation and maintenance.

04 Sangfor anti-ransomware module

- In the field of ransomware protection, ES provides special defense capabilities (layer 4-5-6 protection architecture), and it is displayed on the main page of ES and provide convenient operation guidelines. Sangfor is the most professional vendor in the world in ransomware protection.

POC Guideline

Ransomware protection in all stages of attack

Micro-segmentation traffic visualization and self-generate policies

NGAF & Endpoint Secure integration

One-click quick isolation, entire network threat locating