Sangfor Endpoint Secure

Competitive Analysis Sangfor vs. Bitdefender

www.sangfor.com

SANGFOR

Bitdefender Advantages and Disadvantages Summary

01

Bitdefender is a private software company providing EPP and EDR via their platform, GravityZone Ultra, and a cross-endpoint proxy for endpoints, physical, virtual or cloud servers through cloud or local management.

For organizations that value the accuracy of malware detection, agent performance, and a fully supported data center and cloud workloads from a single solution, Bitdefender is a good choice.

Advantages

01

Bitdefender has a large R&D team that focuses on threat research, and has always maintained excellent malware protection testing performance.

02

Low-overhead EDR is supported by multiple detection layers and automatic response operations, enabling enterprises and mid-market organizations to benefit from EDR.

03

Gartner clients praise Bitdefender for its ease of use, deployment and customer support.

04

Bitdefender provides a series of features that can reduce the endpoint attack surface, including application permission lists. GravityZone provides integrated vulnerability and configuration monitoring, and can provide additional licenses for patch management, in addition to full-disk encryption, web content filtering and device control.

Disadvantages

01

Bitdefender EDR capability lacks numerous common advanced security features. Operations center (SOC) provides analyst workflow, automatic indicator of compromise (IOC) or threat feed integration, custom query and blocking rules, contextual information, and guided investigation.

02

The Bitdefender patch management module, firewall module, and sandbox analysis functions are not yet available on the Linux platform, nor can they inter-operate with other client management tools for repair.

03

Anomaly detection and Bitdefender's MDR are new products that have not yet been verified in the market.

04

The EDR function is only available in the cloud platform. The application permission list function is only available on the local platform. Although Bitdefender has taken steps to expand its corporate influence and sales operations, the sharing of ideas among Gartner customers is still very low.

Sangfor Endpoint Secure vs. Bitdefender

02

Competitive Comparison

	Sangfor Endpoint Secure	Bitdefender
AV Protection		
AI Behavior Analysis	✓	Optional
Signature Database	✓	✓
In-Memory Protection	✓	✓
Fileless Attack Protection	✓	✓
Pre-Execution ML Detection	✓	✓
Phishing Protection	✗	Optional
Anti-Spam Protection	✗	Optional
Application Whitelist	✓	✓
AV Scan CPU Resource Control	✓	✗
On-Premises Sandbox	✓	Optional
Cloud Sandbox	✓	✓
Vulnerability Protection		
Host Based IPS/Firewall	✓	✓
Realtime Vulnerability Scanning	✓	✗
Scheduled Vulnerability Scanning	✓	✗
Rule Based Virtual Patching	✓	✓
Scan Based Virtual Patching	✓	✓
Exploit Detection	✓	Optional

	Sangfor Endpoint Secure	Bitdefender
Detection & Response		
Device Control	✓	✓
DLP	IAG	✗
Realtime Visual Endpoint Connection Analysis	✓	✗
Ransomware Protection (blocking)	✓	Optional
Ransomware Protection (file backup)	Built-in backup feature in HCI	Optional
Ransomware Protection (stop encryption)	✓	✗
One-Click Network-Wide File Kill	✓	Optional
Local Micro segmentation/Isolation	✓	Optional
Network/Remote Micro segmentation	✓	✗
Direct Firewall Integration	✓	✗
Cloud Backup	Built-in backup feature in HCI	✗
Device Support		
Window XP SP3/Vista/7	✓	✓
Windows 8.0/8.1	✓	✓
Windows 10	✓	✓
Windows Server 2003/2008(R2)/2011	✓	✓
Windows Server 2012/2016/2019	✓	✓
Linux	✓	✓
iOS	✗	✗
Agentless (VMWare ESXi)	✗	✗
Management		
On-Premise	✓	✓
Firewall	✓	✗
Cloud	✓	✓
SaaS	✓	✗
Remote Agent Installation	✓	✓
Asset Discovery, Monitoring & Management	✓	✗

	Sangfor Endpoint Secure	Bitdefender
Support Services		
Normal Business Hours	✓	✓
24/7 Phone/Chat Support	Optional	Optional
Malware Removal Service (once)	✓	Optional
Malware Removal Service (unlimited)	Optional	Optional
Security Health Check Service (annual)	✓	Optional
Managed Detection & Response (MDR)	Optional	Optional

How to Win Against Bitdefender - Sangfor Endpoint Secure's Selling Points 03

Sangfor Endpoint Secure Advantages

01 Complete closed-loop capabilities for ransomware prevention, protection, detection and response

- Uses system vulnerability scanning and repair, host micro-segmentation, host security baseline check and repair to prevent intrusion of ransomware.
- Real-time protection against ransomware through use of file directory protection, process reinforcement whitelist, brute force attacking protection, and fileless attack protection.
- Sensitive detection of ransomware provided through multi-engine real-time detection, ransomware decoy trap detection, and active ransomware scanning.
- Emergency response to ransomware through one-click host isolation, ransomware decryption, remote source tracing and evidence collection, and endpoint-network-cloud integration.

02 Efficient response and disposal capabilities

- Sangfor Endpoint Secure detects and responds to events and deals with them quickly by isolating the compromised host with one-click, quickly cutting off the spread of the virus. Endpoint Secure also provides the industry's most innovative micro-isolation functions, convenient and easy-to-configure east-west flow control functions, and visible flow between endpoints in the network.

03 Network endpoint integration capability

- Sangfor Endpoint Secure supports integration with network security products like firewall, Cyber Command and IAM, helping customers realize three-dimensional protection. Network-endpoint integration is a great advantage of Sangfor Endpoint Secure, helping to locate abnormal processes on the host, and respond granularly via network side products, including virus detection and killing, isolation of hosts and files, end processes and blocking ports and IP addresses.

04 Whole network asset inventory

- Sangfor Endpoint Secure supplies statistics and information about all assets and endpoints, from the perspective of the entire network, convenient for clarifying internal network risks and providing a basis for the formulation of security strategies.

05 Engine Zero AI is an efficient and reliable defense

- Engine Zero independently learns to effectively defend against unknown threats, and has a high detection rate among peers in the isolation network environment.

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