![SANGFOR]

SANGFOR ANTI-RANSOMWARE SOLUTION

The Only Solution that Kills Ransomware in 3 Seconds

The Sangfor Anti-Ransomware Solution offers robust and intelligent defense against ransomware. It detects and blocks known ransomware with nearly 100% accuracy and continuously learns new threat patterns to combat zero-day ransomware attacks. Additionally, the solution uncovers hidden threats and ransomware already present in the environment. Equipped with real-time AI-enabled behavioral detection, it guarantees rapid and precise identification with minimal false positives.
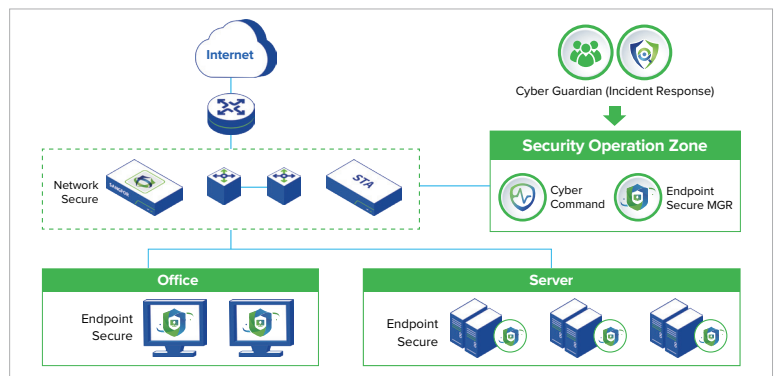
Who It's For ?

Large Organizations

Solution Composition: Endpoint Secure + Network Secure + Cyber Guardian (MDR) + Cyber Command (Optional)
Requirements:
- ✅ Comprehensive protection across endpoints and the network, enhanced with advanced threat intelligence.
- ✅ A single, user-friendly dashboard for efficient management of devices, network, and overall security posture.
- ✅ Real-time file backup that is activated when suspicious encryption occurs.
- ✅ Proactive security services to guarantee a robust defense in the absence of a dedicated security team, including 24/7 continuous monitoring, accurate analysis and investigation to identify ransomware, and assisting with remediation and recovery.

Midsize Organizations

Solution Composition: Endpoint Secure + Network Secure + Cyber Guardian (IR)
Requirements:
- ✅ Comprehensive ransomware protection for both endpoints and the network.
- ✅ Correlating network and endpoint data to enhance the detection of ransomware threats.
- ✅ Real-time file backup that is activated when suspicious encryption occurs.
- ✅ Leverage the expertise of security professionals for effective ransomware response.

Small Organizations

Solution Composition: Endpoint Secure
Requirements:
- ✅ Advanced AI technologies to protect against advanced ransomware on endpoints.
- ✅ Real-time file backup that is activated when suspicious encryption occurs.
- ✅ User-friendly interface, making it easy for non-security experts to navigate and use.

Key Values

Block Ransomware within 3 Seconds

Sangfor Anti-Ransomware rapidly blocks malicious ransomware processes within 3 seconds of execution and alerts the user. In real environment tests with 127 ransomware samples, the solution achieved an average detection and blocking time of 1.53 seconds.

AI-Driven Ransomware Detection

The solution utilizes static and dynamic AI-based detection engines to identify and block ransomware in real time. By collecting ransomware indicators of compromise from over 12 million devices, it achieves an impressive detection accuracy rate of 99.83%.

Ransomware Lifecycle Protection

Pre-attack, the solution employs advanced threat intelligence and behavior analysis for early threat detection and warnings. During attack, real-time monitoring by AI engines swiftly blocks suspicious activities. Post-attack, dynamic backup and one-click rollback mechanisms facilitate rapid restoration of encrypted files, minimizing potential losses.

Intuitive Security Visualization

The solution prioritizes user experience with intuitive dashboards. Security events are mapped with Attack Chain Visualization with an intuitive logical traffic relationship map that displays normal and abnormal connections. Remediation recommendations are provided, suggesting appropriate actions like host isolation, file isolation, or process termination.

Dynamic Backup & One-Click Recovery

Sangfor Endpoint Secure is the world's only endpoint security solution with a built-in ransomware honeypot. By deploying strategically placed bait files, it precisely detects ransomware encryption and triggers immediate backup of user files. Sangfor's unique real-time file-based recovery and snapshot-based recovery ensure that data can be rapidly restored in the event of encryption.