SANGFOR | SANGFOR SECURITY

SANGFOR OMNI-COMMAND

Revolutionize Your Cyber Defense with
Intelligent XDR Solution

Transforming Threat Detection into Intelligent Strategic Defense

In an era of escalating cyber threats, traditional security measures are falling short. We are faced with a stark reality: no security system is completely foolproof, and the consequences of a single breach can be devastating for any organization. The key to robust cybersecurity lies not only in prevention but also in rapid detection and response after a breach occurs. Modern organizations, burdened by disjointed security tools, often find themselves flooded with security alerts. The lack of effective correlation and prioritization of these alerts results in fragmented and inefficient responses. Compounding this issue is the fact that many existing detection and response systems focus narrowly on endpoints, neglecting the threats that penetrate through networks, servers, and more. A truly comprehensive security strategy must integrate detection and response across all potential entry points to establish a holistic security posture.

Sangfor Omni-Command introduces a transformative approach to cybersecurity. A cutting-edge Extended Detection and Response (XDR) platform, Omni-Command breaks the limits of traditional security solutions, offering an integrated and intelligent strategy to combat dynamic cyber threats. Utilizing advanced AI analytics and the groundbreaking Security GPT, Omni-Command converts an overwhelming volume of alerts into precise, actionable intelligence. This capability is crucial in delivering accurate and rapid threat detection and response in today's intricate digital landscapes. Omni-Command not only represents an advanced technological solution but also symbolizes a paradigm shift in how cyber threats are perceived and managed.

The Sangfor XDR Trilogy: Defend, Detect, Response

Defend: Optimal Protection

Implement fast, efficient, and straightforward protective measures. This defense is about swiftly countering threats with minimal complexity, keeping your digital environment secure.

Detect: Maximize Visibility

Gain extensive visibility across your entire organization. This step involves thoroughly monitoring every part of your business, ensuring that no area is left unchecked for potential vulnerabilities and threats.

Response: Single-Click Automation

Use automated, one-click solutions to respond to and recover from security incidents quickly. This simplifies the recovery process, allowing for a rapid return to normal operations.

Redefining Cybersecurity: The New Future of Security with Omni-Command

Revolutionize Your Cybersecurity with Intelligent XDR

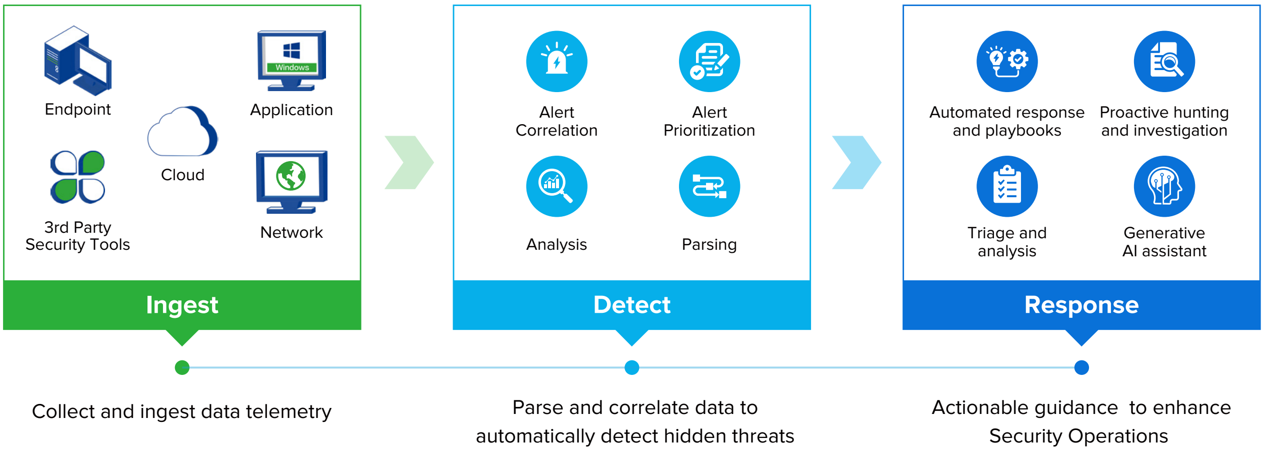
Sangfor Omni-Command stands out as one of the few industry's first on-premises XDR solutions, seamlessly integrating data from various sources, including networks, endpoints, and servers. Omni-Command also offers a versatile SaaS-based model, serving the needs of every organization and cybersecurity strategy.

Omni-Command's integration of Security GPT, a cutting-edge security operations tool based on the Large Language Model (LLM), is a game-changer. It enables security professionals to interact with the platform using everyday language, making advanced security technologies more accessible. This pioneering approach simplifies complex searches, threat analysis, and insight extraction, making these tasks more intuitive and less dependent on specialized cybersecurity knowledge.

The integration of Omni-Command with Security GPT's intelligent alert correlation and incident prioritization cut through the noise, transforming a deluge of alerts into precise, actionable intelligence. As a result, security teams can swiftly access crucial information, cutting down the time spent on investigating, validating, and analyzing security alerts from hours to mere minutes, and focusing on critical incidents.

But Omni-Command's capabilities don't stop there. Its AI-driven analytics not only correlate data across diverse channels but also create comprehensive, easy-to-understand reports that offer deep insights and strategic recommendations. This analytical prowess is the cornerstone for enhancing security postures and refining policies to counteract new cyber challenges effectively.

HOW OMNI-COMMAND WORKS?


Endpoint
Application
Cloud
3rd Party Security Tools
Network
Ingest
Alert Correlation
Alert Prioritization
Analysis
Parsing
Detect
Automated response and playbooks
Proactive hunting and investigation
Triage and analysis
Generative AI assistant
Response
Collect and ingest data telemetry
Parse and correlate data to automatically detect hidden threats
Actionable guidance to enhance Security Operations

Key Components

Omni-Command

Omni-Command is the core component in Sangfor's XDR ecosystem, harnessing the power of artificial intelligence, machine learning, user behavior analytics, and big data. This advanced tool correlates and analyzes data telemetry through a unified platform. Its primary function is to proactively search for hidden threats, identifying them as anomalies in the network and on endpoints, intelligently correlating and consolidating all alerts into clear, contextual, and actionable incidents, achieving a significant reduction in false positives. Omni-Command can be deployed in virtualized environments including Sangfor HCI and VMware.

Sangfor Security GPT

At Sangfor, our AI-first strategy has culminated in our latest innovation — Security GPT, a cutting-edge tool designed for enhanced detection accuracy and operation efficiency. It plays a crucial role in expediting investigation processes, threat hunting, and incident responses. Security GPT is offered in two options: Detection GPT and Security Operation GPT, each tailored to specific functions.

Detection GPT

Detection GPT is engineered to significantly improve the detection rate of various cyber threats, including zero-day attacks, ransomware, and fileless attacks. Its advanced algorithms are purpose-built to recognize and respond to these sophisticated threats, ensuring robust protection against emerging cyber challenges.

Security Operation GPT

This component is split into two key functionalities – Assisted Operation GPT and Auto Operation GPT.

Assisted Operation GPT

This functionality offers interactive support similar to chatbot interfaces. Users can enter queries in natural language, such as asking for the top five security incidents of the week, and receive detailed responses. This dialogue-based interaction supports SecOps teams by providing quick and easy access to vital information.

Auto Operation GPT

This functionality autonomously investigates and analyzes security alerts. It provides logical assessments explaining why certain alerts are categorized as security incidents and their potential harm. Furthermore, it can automatically respond to threats, initiating preventive actions to avert costly data breaches or damage.

Neural-X Threat Intelligence

Sangfor Neural-X is an advanced cloud-based threat intelligence and analytics platform powered by AI. It is continuously with real-time threat intelligence of malicious patterns and behaviors from extensive well-established sources including VirusTotal, IBM X-Force, AlienVault OTX, EmergingThreats.net, Abuse.ch, and more. Additional components like deep learning, botnet detection, sandboxing, and file reputation ensure that all Sangfor security products remain effective against advanced and emerging threats.

Endpoint Secure

Sangfor Endpoint Secure is a modern endpoint protection solution that is powered by Sangfor AI malware detection engine, Engine Zero, to identify and respond to malware on PCs and servers. Omni-Command ingests data from Endpoint Secure to uncover threats through monitoring key user and system activities like process termination, DNS queries, file creation, port monitoring, scheduled tasks, service creation and deletion, and more.

The powerful built-in analysis engines in our Endpoint Secure like AI intelligence, Behavior Analysis, and Gene Engine provide an added layer of protection, along with specific engines to guard against ransomware and fileless attacks.

The introduction of Security GPT by Sangfor represents a significant advancement in the field of cybersecurity, blending advanced AI capabilities with user-friendly interfaces to offer a comprehensive, automated, and highly responsive security solution.

The 5 Key Features of Omni-Command

1. Complete Visibility Across the Entire Environment

Omni-Command offers extensive visibility by ingesting data from network, endpoint, and server environments for correlation and analysis, eliminating any blind spots. The solution's ability to incorporate data from third-party security tools further extends its visibility. This comprehensive surveillance allows for a more thorough understanding of security alerts, consolidating them into singular, actionable incidents. This is essential for exposing hidden threats, vulnerabilities, and shadow IT threats, enhancing the overall security posture.

2. Precise Threat Detection with AI and Behavioral Analytics

Omni-Command leverages big data analytics and AI-driven analysis engines to effectively uncover stealthy cyber-attacks. The AI analysis engines continuously learn typical network behaviors to identify deviations that could indicate security breaches. This evolving capability is crucial in detecting complex threats like zero-day attacks, advanced persistent threats (APTs), and more. Omni-Command’s adaptive ML algorithms are designed to incorporate real-time threat intelligence, ensuring up-to-date defenses against emerging cyber threats.

3. Efficient Threat Hunting with Deeper Analytics

Threat hunting is an integral part of security operations. Omni-Command facilitates this process through its advanced search capabilities, supporting both precise and open-ended queries. This function enables teams to detect suspicious activities by searching for specific hosts, files, processes, registry updates, network connections, and more. By combining threat intelligence with comprehensive data across networks and endpoints, Omni-Command empowers teams to quickly identify ongoing or past attacks.

4. Rapid Investigation of Alerts with Generative AI Assistant

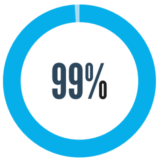
Omni-Command facilitates alert management and investigation with features such as a centralized alert dashboard for efficient sorting, filtering, and investigating, along with root cause and timeline analysis views for in-depth incident examination. These features streamline complex event analysis and decision-making processes. Additionally, the integration of Security GPT in Omni-Command allows security professionals to interact with the system using everyday language, simplifying searches and threat analysis and shortening investigation times from hours to minutes.

5. AI-Driven Incident Response

Omni-Command empowers rapid containment and response to cyber threats, offering security teams the ability to swiftly neutralize threats across networks and endpoint environments from a single, unified console. The platform enables immediate actions to stop malware spread and restrict network activities, utilizing either its preloaded playbook policies or integrating with third-party security tools.

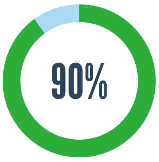
The incorporation of Security GPT enhances these capabilities, ensuring responses are not only quick but also tailored to the specific nature of threats. By simply inputting prompts or instructions to Security GPT, the incident response process becomes automated. For instance, upon detecting a threat, Omni-Command can automatically activate predefined protocols like isolating compromised systems or applying necessary patches, thus drastically reducing response times and minimizing potential damages. This automation of workflows significantly eases the load on security teams, enabling them to concentrate on more complex security challenges.

Key Performance Benefits of Omni-Command



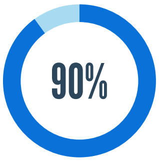
99% Threat Detection in 5 Minutes:

Omni-Command showcases outstanding efficiency in threat detection, accurately identifying 99% of threats within just five minutes. Such swift and accurate detection is crucial in protecting the digital environment against the most sophisticated and unknown threats.



90% Reduction in Alert Volume:

Omni-Command enhances the context for threat detection and significantly minimizes false positive alerts by 90% by integrating data from networks, endpoints, and various third-party security tools. By correlating and consolidating alerts into single, actionable incidents, Omni-Command expedites both decision-making and the identification of threats.

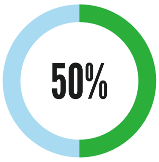


90% Faster Investigation Time:

Omni-Command delivers a 90% reduction in investigation time for cybersecurity incidents, offering a significant upgrade to traditional, time -consuming manual methods. The integration of Security GPT further streamlines operation by allowing security professionals to use simple language for queries and analyses, reducing the time spent on investigations from hours to minutes.

70% Increase in Security Robustness:

Omni-Command enhances system security by 70% by integrating disparate security tools. This integration allows analysts to prioritize high-risk threats more effectively, while the platform’s built-in analytics automatically detect more elusive threats, significantly easing the workload of security teams.



50% Reduction in Security Operation Costs:

Implementing Omni-Command results in a 50% decrease in total deployment and personnel costs related to security operations. This cost-efficiency is achieved by offering a broad range of native functionalities, allowing organizations to consolidate their security stack with a single vendor. Additionally, for environments with diverse security tools, Omni-Command's open integration capabilities enable efficient data unification across various platforms, further enhancing operational efficiency and cost-effectiveness.

Why Omni-Command?

1 On-Premises XDR Deployment Model

True On-Premises Deployment Model	Local Data Residency Assurance	Extended Data Retention
Sangfor Omni-Command is available in both on-premises and SaaS deployment models, distinguishing it in a landscape where many providers focus on SaaS-based solutions. This flexibility is particularly appealing to organizations that prefer local deployment for their cybersecurity infrastructure.	By deploying on-premises, we ensure that all data remains within the country of operation. This is crucial for organizations that need to comply with local data residency laws and regulations, as it prevents the transfer of sensitive data outside national borders.	Our platform supports a default data retention period of 180 days, significantly longer than many standard offerings. This extended retention allows for more thorough collection, correlation, and analysis of security data across various domains within a central repository. This capability is vital for in-depth security analysis and historical threat assessment.

2 Unmatched Threat Prevention

All-encompassing Threat Mitigation	Cross-Platform Protection
Employs cutting-edge machine learning, behavior-based protection, and mitigation techniques against exploits to neutralize advanced threats such as zero-day attacks, APTs, fileless attacks, and more.	Shares protective strategies across networks, and endpoints, reinforcing overall security.
Wide-Ranging Attack Detection and Mitigation	**Highly Accurate Threat Identification**
Offers thorough detection and response capabilities across networks, endpoint environments, and third-party security tools, ensuring no threat is overlooked.	Boasts an impressive daily detection rate, essential for preventing ransomware and data breaches.

3 Advanced Detection of Sophisticated Attacks with Powerful AI and Machine Learning Engines

Complete Threat Detection Coverage	Innovative AI and Analytics Application
Eliminates security blind spots across networks and endpoints environments.	Utilizes machine learning, big data analytics, and Security GPT for enhanced network threat detection and reduced false positives.
Alignment with MITRE ATT&CK Framework	**Customizable Detection Capabilities**
Adapts attack detection strategies in line with the MITRE ATT&CK framework, providing rich contextual information and detailed detection insights, helping security analysts quickly comprehend and respond to threats.	Continual enhancement through customizable rules. This includes the customization of Indicators of Compromise (IOCs) like file hashes, IP addresses, or domain names, and Indicators of Attack (IOAs), such as specific processes initiating others, and more.

4 Simplify Incident Investigation and Response

Smart Alert Consolidation	Unified Data Analysis	Coordinated Attack Containment
Transforms multiple related alerts into singular incidents for more efficient management.	Integrates diverse data sources for a unified view, streamlining the analytical process.	Offers rapid containment and forensics capabilities for swift threat mitigation.

AI Generative Assistant	Swift Attack Source Identification
Security GPT allows users to conduct searches, analyze threats, and extract insights using everyday language, making the platform more accessible and intuitive.	Automates the analysis of attack origins and progression, revealing root causes with ease. It provides detailed incident information, including affected hosts, indicators of compromise, and timelines.

5 Automated Incident Response

Pre-Configured Incident Management

Includes ready-to-use playbooks for Include ready-to-use playbooks for incident responses, enabling automated actions across multiple security tools.

Flexible Third-Party Integration

Provides seamless integration with third-party security tools for comprehensive incident management through API connectivity.

AI Automated Incident Response

Security GPT enhances incident response capabilities, ensuring responses are not only quick but also tailored to the specific nature of the threats. By simply inputting prompts or instructions to Security GPT, the incident response process becomes automated, such as initiating predefined protocols like isolating compromised systems or applying necessary patches, thus drastically reducing response times and minimizing potential damages.

6 Centralized Management of Security Incidents

Comprehensive Security Overview

Aggregates all security alerts for a centralized, context-rich overview throughout the incident response process.

Streamlined Security Alerts

Reduces the volume of alerts, focusing on delivering precise, high-priority notifications to alleviate operational strain. The integration of Security GPT in Omni-Command allows security professionals to interact with the system using everyday language, simplifying searches and threat analysis.

Customizable Analysis Dashboards

Omni-Command features customizable dashboards and reports, enabling in-depth analysis of incidents, indicators, and analyst activities. Its AI-driven functionality analyzes security data thoroughly, producing comprehensive reports that shed light on an organization's overall security posture, emerging trends, and potential vulnerabilities. These detailed insights are invaluable for strategic decision-making, guiding organizations in reinforcing their security frameworks and refining their policies. This capability of Omni-Command to provide tailored, insightful analytics makes it a vital tool for enhancing and maintaining robust cybersecurity measures.

SANGFOR OMNI-COMMAND

INTERNATIONAL OFFICES

SANGFOR SINGAPORE
10 Ubi Crescent, #04-26 Ubi
Techpark (Lobby B), Singapore 408564
Tel: (+65) 6276-9133

SANGFOR HONG KONG (CHINA)
Unit 1612-16, 16/F, The Metropolis Tower,
10 Metropolis Drive, Hung Hom, Kowloon, Hong Kong
Tel: (+852) 3845-5410

SANGFOR INDONESIA
Atrium Mulia 3rd Floor, Jl. H.R. Rasuna Said Kav.
B 10-11 Kuningan, Setia Budi, Kecamatan
Setiabudi, Kota Jakarta Selatan, Daerah Khusus
Ibukota Jakarta 12910, Indonesia
Tel: (+62) 21-2168-4132

SANGFOR MALAYSIA
No. 45-10 The Boulevard Offices,
Mid Valley City, Lingkaran Syed Putra,
59200 Kuala Lumpur, Malaysia
Tel: (+60) 3-2702-3645

SANGFOR THAILAND
141 Major Tower Thonglor (Thonglor10)
Floor 11 Sukhumvit Road, Kholngtan Nuea
Wattana BKK, Thailand 10110
Tel: (+66) 02-002-0118

SANGFOR PHILIPPINES
Unit 14B 14th Floor, Rufino Pacific Tower,
6784 Ayala Avenue, Makati City, Metro Manila,
Philippines
Tel: (+63) 916-267-7322

SANGFOR VIETNAM
210 Bùi Văn Ba, Tân Thuận Đông, Quận 7,
Thành phố Hồ Chí Minh 700000, Vietnam
Tel: (+84) 903-631-488

SANGFOR SOUTH KOREA
Floor 17, Room 1703, Yuwon bldg. 116,
Seosomunro, Jung-gu, Seoul, Republic of Korea
Tel: (+82) 2-6261-0999

SANGFOR UAE
D-81 (D-Wing), Dubai Silicon Oasis HQ Building,
Dubai, UAE
Tel: (+971) 52855-2520

SANGFOR ITALY
Floor 8, Via Marsala, 36B, 21013 Gallarate VA, Italia
Tel: (+39) 0331-6487-73

SANGFOR PAKISTAN
Office No.210, 2nd Floor, "The Forum",
Plot No. G-20, Block 9, Khayaban-e-Jami, Clifton,
Karachi, Pakistan
South Region: +92 321 2373991
North Region: +92 345 2869434
Central Region: +92 321 4654743

SANGFOR TÜRKIYE
A Blok. Kat 51. D 643, Atatürk Mh, Ertuğrul Gazi Sk,
Metropol İstanbul Sitesi. 34758 Ataşehir/İstanbul
Tel: (+90) 216-5156969

AVAILABLE SOLUTIONS

IAG - Internet Access Gateway
Secure User Internet Access Behaviour

Network Secure - Next Generation Firewall
Smarter AI-Powered Perimeter Defence

Endpoint Secure - Endpoint Security
The Future of Endpoint Security

Cyber Command - Network Detection and Response
Smart Efficient Detection and Response

Omni-Command - Extended Detection and Response
Revolutionize Your Cyber Defense with Intelligent XDR

TIARA - Threat Identification, Analysis and Risk Assessment
Smart Threat Analysis and Assessment

IR - Incident Response
Sangfor Incident Response – One Call Away

Cyber Guardian - Managed Threat Detection & Response Service
Faster Response Through Human/AI Collaboration

HCI - Hyper-Converged Infrastructure
Fully Converge Your Data Center

MCS - Managed Cloud Services
Your Exclusive Digital Infrastructure

VDI - aDesk Virtual Desktop Infrastructure
Seamless Experience, Secure and Efficient

Access Secure - Secure Access Service Edge
Simple Security for Branches & Remote Users

EDS - Enterprise Distributed Storage
The Only Secured Data Storage You Need

SD-WAN
Boost Your Branch with Sangfor

Sales: sales@sangfor.com

Marketing: marketing@sangfor.com

Global Service Center: +60 12711 7129 (or 7511)

www.sangfor.com