# SANGFOR SIMPLIFIED SECURITY OPERATIONS SOLUTION

Simply Your Security Operations

The Sangfor Simplified Security Operations equips organizations with a systematic and future-proof security fabric by integrating Sangfor and third-party security products and services. It enhances **the effectiveness and efficiency of daily security operations,** including risk and asset management, threat and incident detection, and response. The solution empowers security teams to tackle various challenges, from managing massive alert volumes to handling complex investigations.
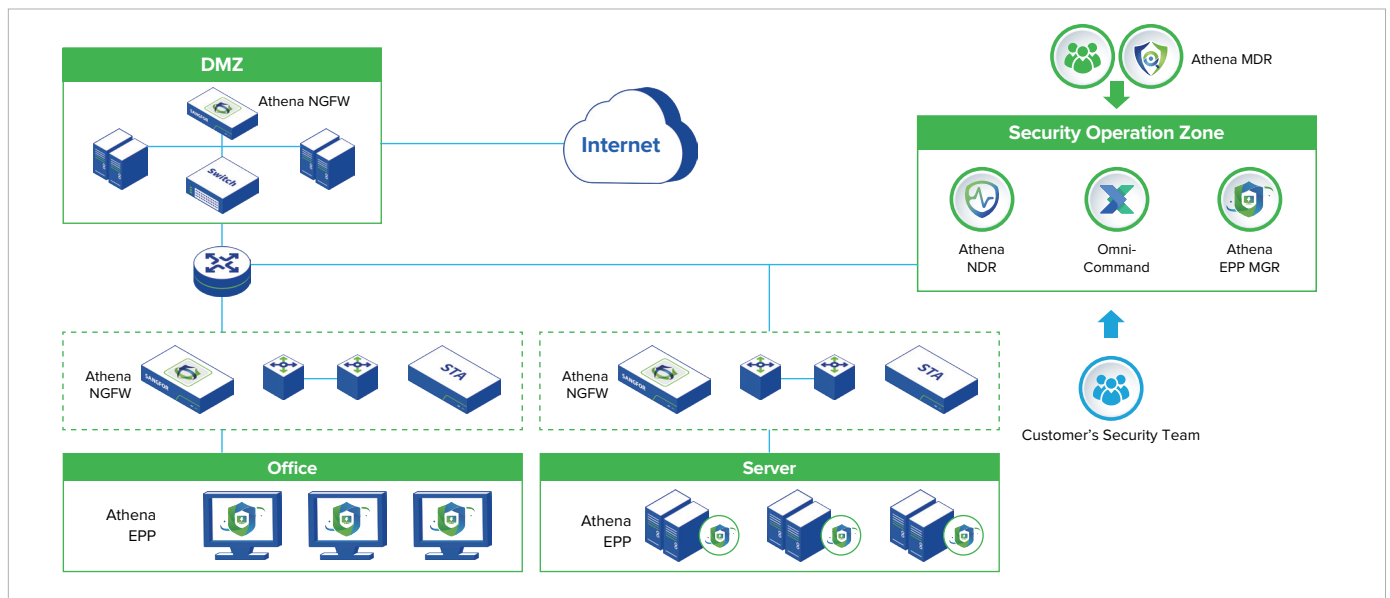
Who It's For ?

Large Organizations

- ✓ Solution Composition: Omni-Command + Athena NDR (STA sensor only) + Athena EPP + Athena NGFW + Athena MDR.
- ✓ Often subject to both internal and external regulations.
- ✓ Follows mature security frameworks (e.g., NIST and CSMA) and clear security operations processes.
- ✓ Comprehensive security setup including SIEM, network and endpoint security, and services.
- ✓ Dedicated information security function led by a CISO.
- ✓ The security team mainly focuses on daily alert investigations, correlating data across different tools, and reporting to management on a monthly or quarterly basis.

Midsize Organizations

- Solution Composition: Athena NDR + Athena EPP + Athena NGFW + Athena MDR
- Generally resource-constrained and struggles with correlation analysis between different security products.
- Lacks the means to detect stealthy threats, such as risky internal practices, irregular traffic patterns, and hidden malware.
- Wants visibility of the entire security infrastructure to understand the entry points of attacks and the attacker's activities.
- Usually has security products for network or endpoint protection.
- Unable to permanently remediate security incidents, often needing to repeat response actions.

Key Values

Consolidated Security Infrastructure

The solution builds upon your existing security architecture through integration and correlation with other security products. It creates a systematic and unified security ecosystem with integrated defense capabilities, rather than having each product operate in isolation.

Streamlined Security Alert Analysis

Eliminate the need to manually correlate and sift through thousands of logs across various security components to identify malicious activities. Enjoy unified management, reporting, triage, and response—all on a single platform. Alternatively, access the information you need by asking our GenAI assistant, Security GPT.

Credible and Reliable Security Assurance

The solution alleviates concerns about skill or staff shortages by providing flexible security services to support your security operations. These services include rapid business recovery, root cause analysis, regular threat and risk assessments, and managed detection and response, ensuring comprehensive security management.

Bringing Security Alive with GenAI

Security GPT's AI engine continuously evolves with ongoing data input and refinement by Sangfor's security experts. It imparts intelligence to security components, significantly improving their ability to detect threats and cyberattacks.

- **Peak Processing performance:** 50 times faster than the original GPT, enabling real-time processing
- **Advanced Cyberattack Detection:** High true positive rate and zero-shot generalization capability
- **SecOps "AutoPilot":** Requires minimal manual interaction and skills