SANGFOR SECURITY BUTLER

Simplify Your Security Operation with Butler Level Service

Taking Care of Details While You Take Care of Business

Global cybercrime is predicted to reach more than $2.1 trillion in 2019 and cyber-threats don't take days off. Sangfor Security Butler, a Cloud-based Security Operation Center, makes end to end, expert-level security operation a luxury that everyone can afford. Security Butler performs complex firewall log reviews and correlation, alert and highlight relevant and critical security incidents for administrators and enables quick emergency response, all from the convenience of a cloud-based portal 24 hours a day, 7 days a week.

Current Challenges

It takes an average of 200 days for an organization to detect a security breach. Quicker time to detection enables a company to minimize damage and to stop potential data breach. However, security operation requires a team of security experts to operate 24/7 while companies of average size often lack the sufficient IT security skillset, visibility or budget to conduct comprehensive security operations, leaving them extremely vulnerable to attack.

- Customers often perform firewall review very infrequently (weekly or monthly) – or don't conduct proactive security operations at all, which lead to a lack of visibility and timely response to critical security breaches.
- Large enterprises recognize the importance of SecOp. They either have their own SecOp team or outsource this task to MSS. However, this practice is prohibitively expensive, as qualified Security Analysts is costly, in high demand and rarely available on a 24/7 basis.

Security Operation Requires Expertise & Budget

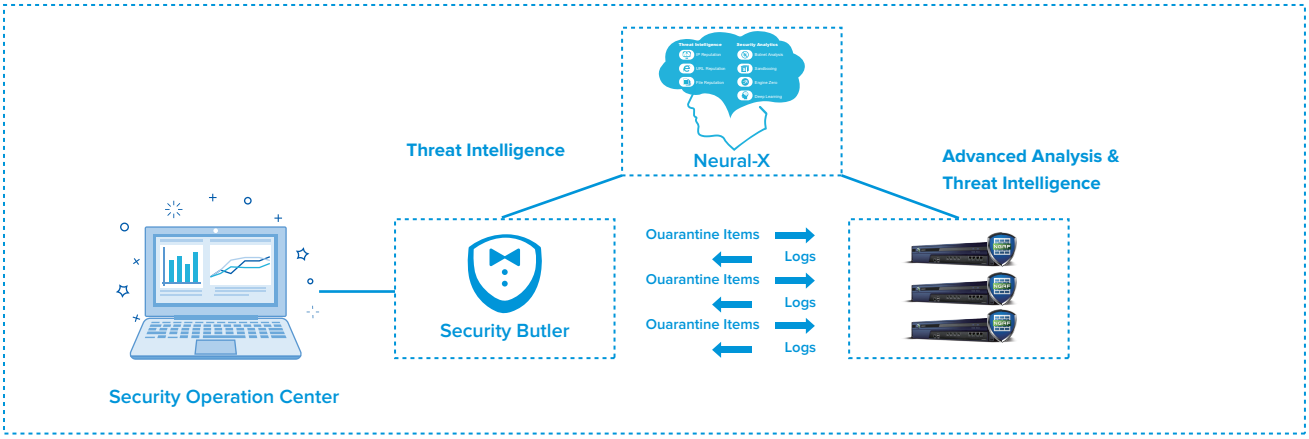
- **Trouble Tickets**
- **Process Alerts**
- **Vulnerability Assessment**
- **Log File Reviews**
- **Security Events**
- **Treat Correlation**
- **Maintenance Management**
- **Research IOC on TI**

What is Sangfor Security Butler?

Your Own Cloud-Based Security Operation Center:

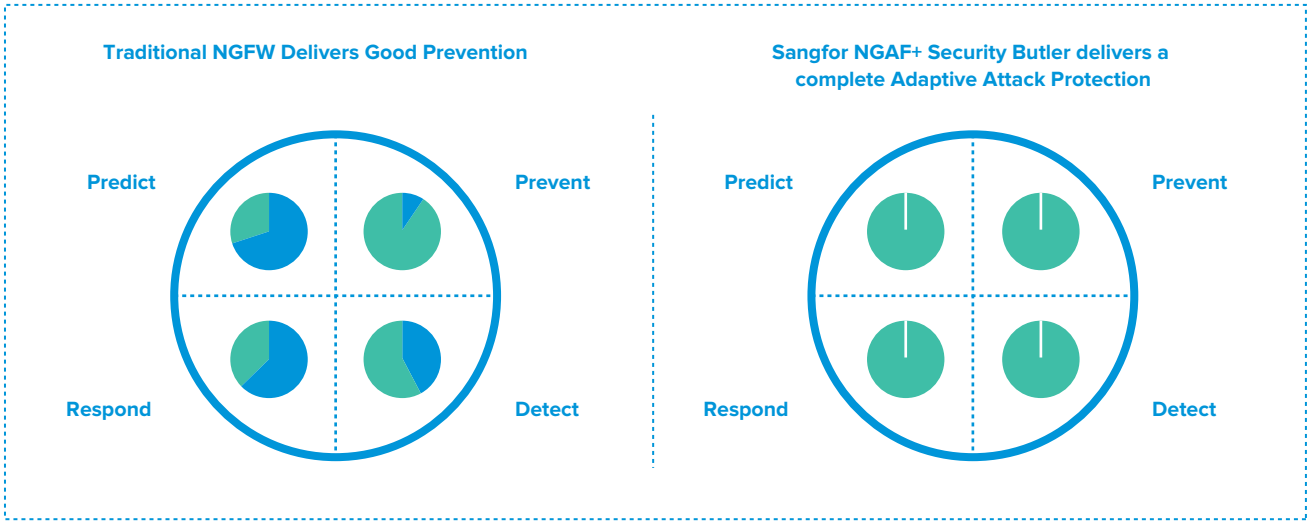
- Security Butler performs 24/7 time-consuming firewall log reviews on your behalf.
- Real-time risk detection to highlight relevant and critical security incidents.
- Improve your overall risk posture by tasking Security Butler with performing basic incident response & quarantine of compromised assets.

How Does It Work?



- Security Butler requires Neural-X, an AI Enabled Cloud Platform for Threat Intelligence & Analytics developed by Sangfor Technologies.
- All participating Sangfor NGAF firewalls collectively share their logs with Security Butler. All logs are securely stored with multi-tenancy, designed to ensure privacy.
- Security Butler performs automated processing, correlation and TI look up, as well as human processing on the back end. Logs from customers or partners who have multiple firewalls under management are correlated.
- Security operation teams have access to their own Security Butler portal.
- The Security Butler portal gives users access to Advanced Threat Protection (including APT & Ransomware attacks, webshell events, etc), Asset Security Analysis (vulnerable business systems, targeted hosts, etc.) and Threat Intelligence.
- SecOps can directly block or quarantine certain assets from Security Butler.

Protection Against Advanced Threats

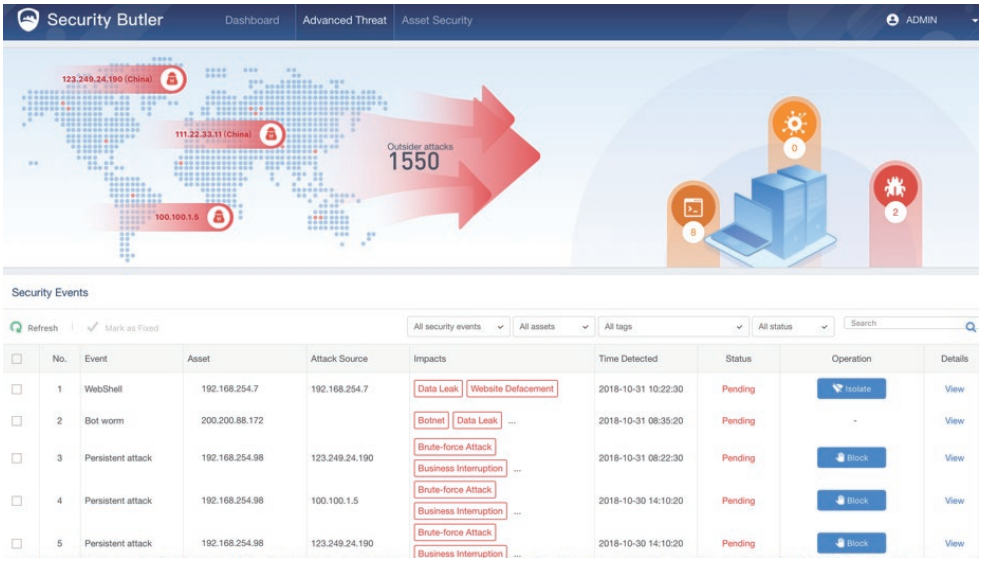


Security Butler analyzes the entire network security log through an advanced threat model base on cloud big data, identifying high-risk external attacks and internal fault events in the user's network. Alarms are sent to the administrator via email in real-time, so the user is aware of any existing advanced threats in the network in a timely manner.

At the same time, the Security Butler works together with Sangfor NGAF to block IP addresses and network disconnection responses, helping users deal with advanced threats and avoid loss of assets.

Advanced threat events include:

- Advanced Hacker based on techniques, persistency, attack duration as well as TI look up
- APT
- Webshell
- Botnet Virus
- Virus/malware Infection



Highlights

Since the release of Security Butler, many customers have seen their complex and time consuming daily security operation transform into an ultra-simplified task. “Previously, it took us at least 2 hours to check the firewall status, security logs and threat status. After implementing Security Butler, we have reduced the overall time to 10 minutes, allowing our team to focus on other critical tasks.” says the IT Manager of a large Chinese Automobile Manufacturing company managing more than 4 Sangfor NGAF firewalls.

Fully Visibility of Security Events

- Customized Security Policies
- Expert Security Level
- 24/7 Monitoring

- Real-time active Response
- Professional Security

- Expert Online Assistance
- Unified Security Management

Customer Benefits With Security Butler

Item	With Security Butler	Without Security Butler
Security Log Review	Minutes	Hours
Security Monitoring	24/7	Oniy when resource allows
Security Event Priority	Automatic	Manual
Security OPEX	Lower	Higher