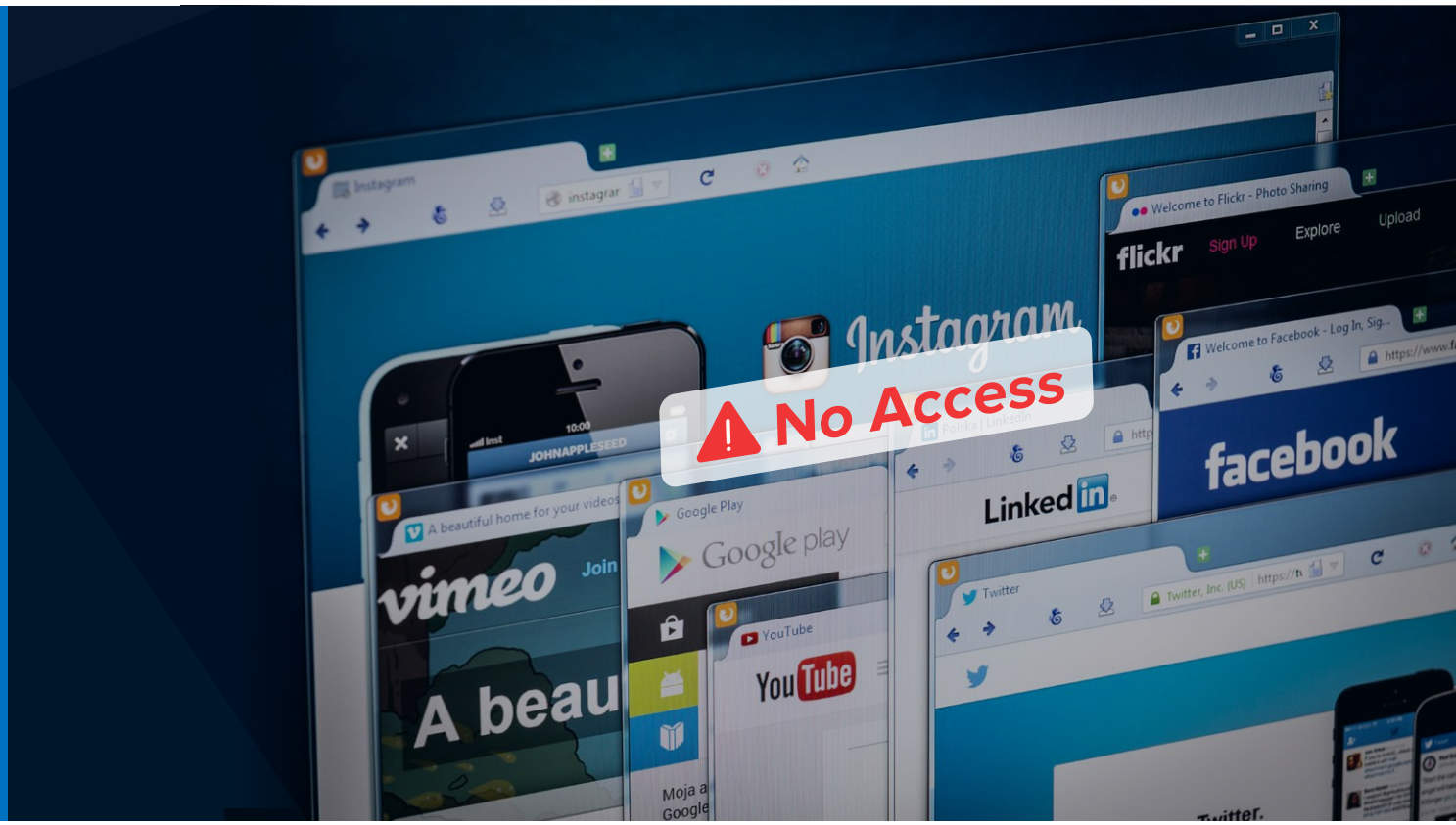
SANGFOR

SANGFOR XDDR

Application Containment Solution

Sales Guide



CONTENTS

1. Introduction

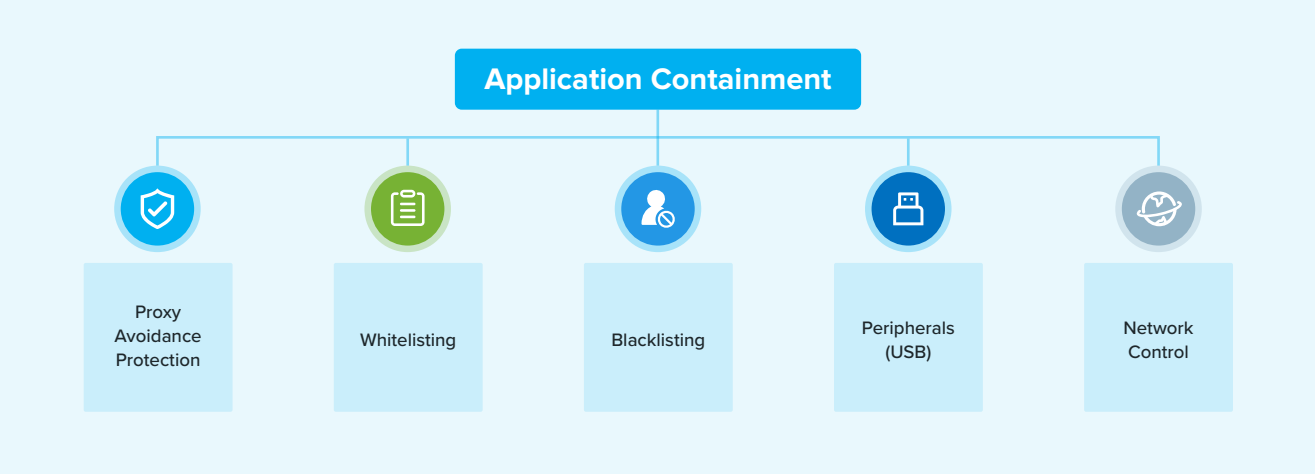
This sales guide is provided to help the user understand how to sell the Sangfor Application Containment Solution.

2. Why is it Application Containment/Proxy Avoidance Protection important?

XDDR Application Containment Solution is designed to give administrators granular control of applications running on endpoints, servers, and across the network. Only allowing authorized applications on systems and the network reduces the potential for malware, ransomware, and APT infection. The Proxy Avoidance Protection use case will improve employee productivity and reclaim squandered bandwidth within the organization.

3. Application Containment Use Cases

Application Containment has 5 use cases:



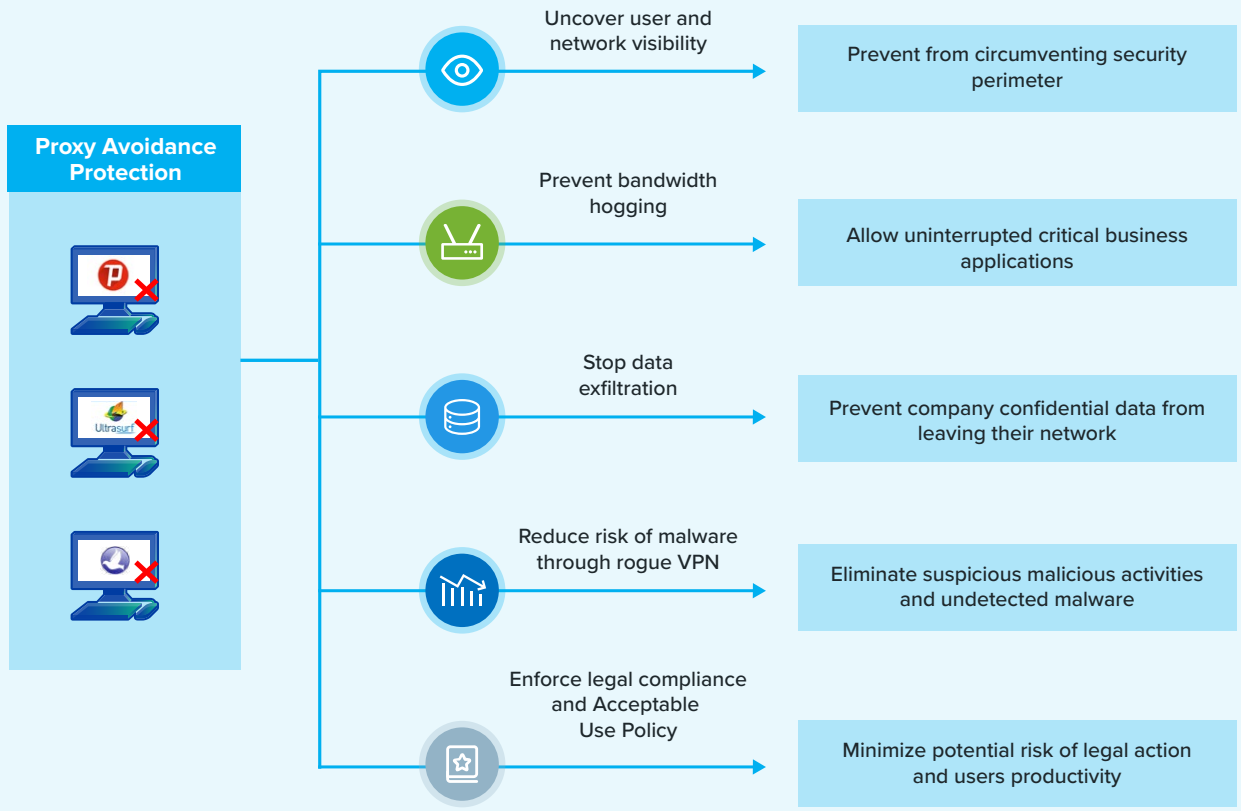
• **Proxy Avoidance Protection** has a library of well-known anti-proxy applications, anonymous browsers, and VPNs to create blocking/monitoring policies enforced by the Endpoint Secure Protect Agent.

• **Whitelisting/Blacklisting** can be implemented by selecting from the running applications reported to the NGAF by Endpoint Secure.

• **Peripheral Control** manages access to USB devices such as portable drives, thumb drives, mobile devices, cameras, etc. Allowed devices can be whitelisted.

• **Network Control** enables Endpoint Secure to send port and connection information to NGAF where it can block malicious connections such as malware command & control communications or lateral propagation of malicious software.

Why Proxy Avoidance Protection and How Can It Help You?



4. Sangfor Application Containment Value Proposition

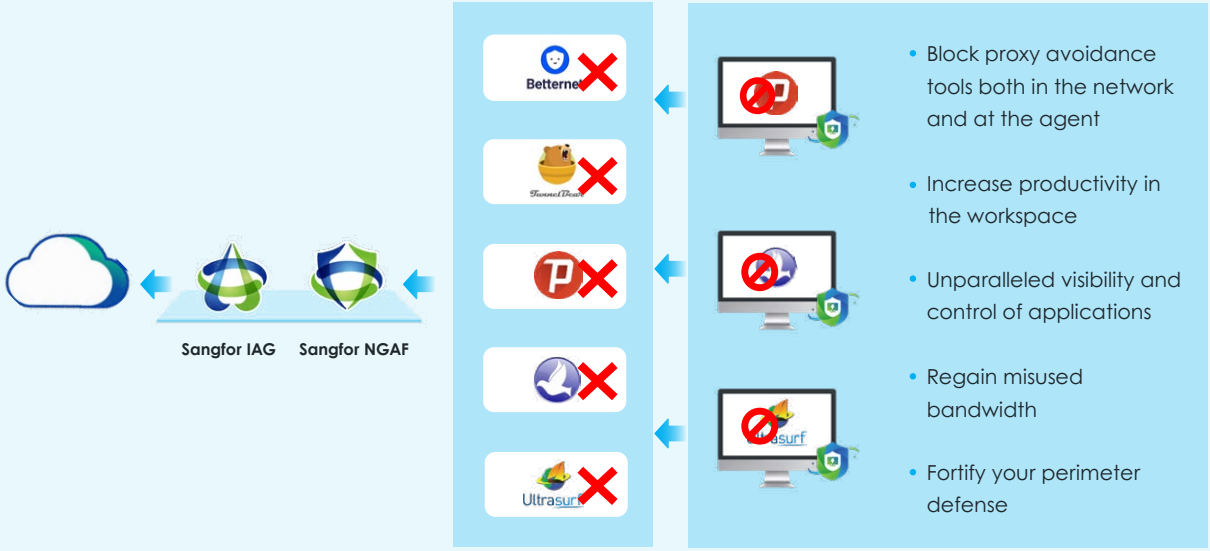
Application Containment has two main value propositions:

WFX

- Prevent infection of WFX systems by blocking unauthorized applications from starting or allowing only whitelisted applications to start.
- Prevent breached WFX systems from infecting or attacking corporate resources through VPN using IAG.

Proxy Avoidance Protection From Internal Users

- Block proxy avoidance tools both on the network using IAG and on endpoints using Endpoint Secure.
- Increase productivity in the workspace by blocking unauthorized social media apps, instant messaging (IM). or chat apps, and games
- Regain misused bandwidth by blocking cryptomining apps, streaming media players, and online games.
- Unparalleled visibility and control of running applications using the NGAF Security Management Dashboard.



5. Sangfor Application Containment Key Features

1. Simple XDDR integration and management between Endpoint Secure with NGAF or IAG
2. Comprehensive library of Proxy Avoidance applications including VPNs, anonymous browsers, and proxy circumvention applications
3. Flexible deployment options using inline gateway or bridge modes
4. Easy whitelisting/blacklisting of applications
5. Block unauthorized applications from starting on endpoint
6. Block network communications from unauthorized applications
7. USB peripheral control to prevent access to removeable & portable drives, thumb drives, and mobile devices

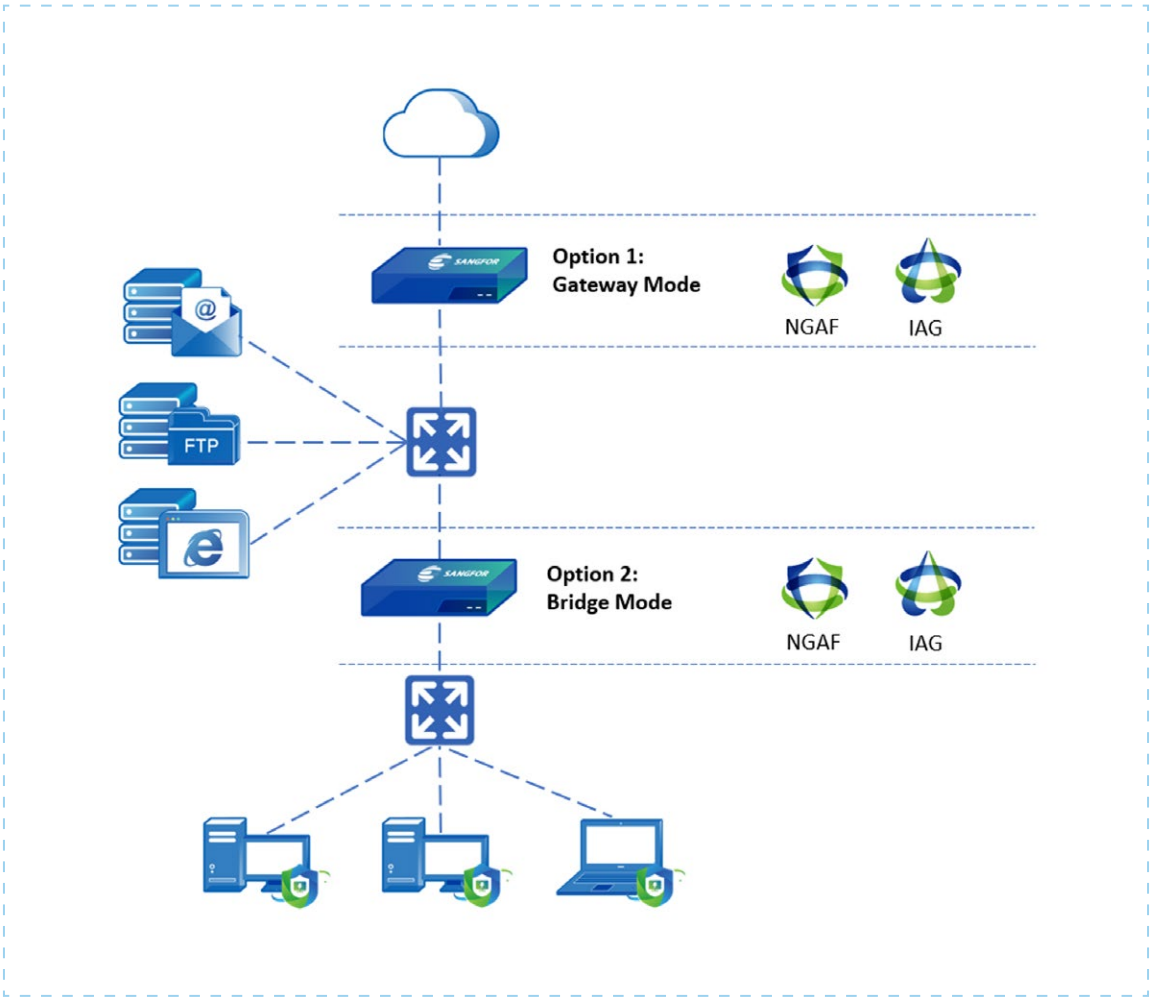
6. Feature Matrix (IAG vs NGAF)

Feature	NGAF	IAG
Max endpoint	The application containment policy only applies to 2000 endpoints. Any endpoints over 2000 will not be controlled.	10,000 endpoints based on Endpoint Secure Manager.
Supported Endpoint Secure Integration	On Premise & Cloud Endpoint Secure.	On Premise Endpoint Secure only (cloud supported in later release).
Reporting	NGAF provides dashboard to show the blocking status but does not include any reporting or logging.	Dashboard and internal reporting center. User detail provided (username, group, endpoint device, etc.).
Deployment option	Bridge, Gateway	Bridge, Gateway
Other application control	• Proxy/VPN Tools. • Non-system applications.	Proxy Avoidance Protection.
Configuration	• Connect NGAF to Endpoint Secure Manager (on-premises, cloud). • Configure & Deploy policy from NGAF. • Blocking via Endpoint Secure.	• Connect IAG to Endpoint Secure Manager (on-premises, cloud) • Configure & Deploy policy from IAG • Blocking via Endpoint Secure and IAG (network)
Policy Rollback	Yes	Yes
Browser extension blocking	On roadmap	On roadmap
Dashboard	Display data for max 2000 endpoints.	Display 30,000 entries or last 7 days, whichever is greater.
Application Signatures Update	Every 2 weeks	Every 2 weeks

Feature	NGAF	IAG
Integrated Endpoint Secure/ IAG Ingress agent	N/A	On roadmap
Endpoint Offline support	Application Containment still effective even when endpoint is not connected to a network.	Application Containment still effective even when endpoint is not connected to a network.

7. Deployment Options

Both NGAF and IAG support Application Containment in both Gateway and Bridge Modes. Out of band and Monitoring Modes are not supported.

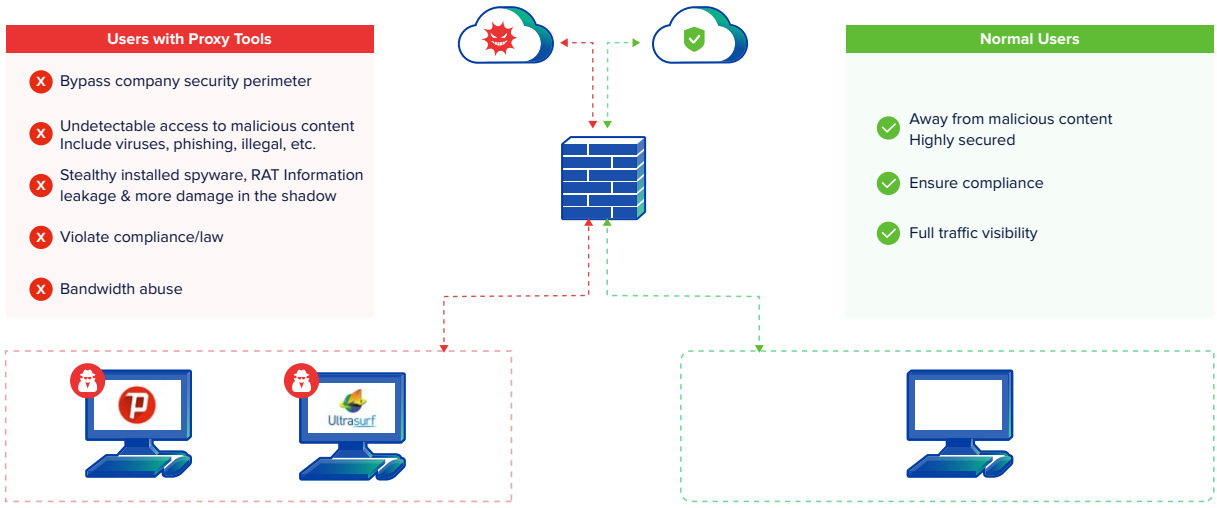


8. Competitive Analysis

Use Case	Sangfor IAG	Sangfor NGAF	Symantec (Broadcom)	Allot	FortiGate	Sophos XG	Remarks
Proxy Avoidance Applications Signature	Strong	Strong	Strong	Strong	Strong	Strong	Sangfor constantly researches and generates updates for the top 50 proxy avoidance applications, including anonymous proxy and rogue VPNs. In contrast, other competitors have equivalent lists of PAP applications but lack consistent updates. Some competitors' most recent updates are dated 2020.
Gateway protection Efficacy	Strong	Strong	Weak	Weak	Weak	Weak	Sangfor has high efficacy detecting and blocking proxy avoidance applications based on web access. Most competitors do not have this capability.
Integration with Endpoint	Strong	Strong	Average	Weak	Average	Strong	Sangfor can detect and block with pinpoint accuracy any locally installed proxy avoidance applications. Some competitors' integrated endpoint offerings emphasize XDR but are weak on similar PAP integration with endpoint.
Whitelisting	Average	Strong	Average	Weak	Average	Strong	Sangfor IAG non-PAP application whitelisting limited to domain and IP address.
Blacklisting	Average	Strong	Average	Weak	Average	Strong	Sangfor IAG non-PAP application blacklisting limited to domain and IP address. Current IAG Ingress agent has similar capabilities to NGAF/Endpoint Secure for blacklisting running processes, files, and registry-based rules.
Peripherals (USB)	Strong	Strong	Weak	Weak	Weak	Weak	Sangfor has a wide range of peripheral control including storage, network, mobile, and Bluetooth devices as well as camera and printer. Whitelisting can be configured by hardware device ID and auto-discovery of recently used storage devices.
Network control	Strong	Strong	Weak	Weak	Weak	Weak	Sangfor IAG has similar capabilities to NGAF/Endpoint Secure using Ingress Client to perform endpoint compliance security verification based on anti-virus software/database, login domain, operating system, access control, local windows account, etc.

9. Target Customer

Who Do We Sell To & Why?



Existing NGAF Customer

1 Government

Pain points

- Slow Internet connectivity and unable to prioritize bandwidth for critical business applications.
- Circumvention of security perimeter allows unrestricted access to unauthorized or illegal Internet activities.
- Unintentional or malicious users expose confidential data via proxy avoidance applications.
- Potential legal action based on illegal use or access.

Benefits

- Eliminate use of proxy avoidance applications
- Gain back control of bandwidth management
- Restore visibility and control over user internet activity and productivity
- Prevent confidential data from leaving network
- Enforce legal compliance and Acceptable Use Policy (AUP)

2 Enterprise/SMB/SME

Pain points

- Staff accesses non-work-related applications/website impacting work efficiency
- Expensive bandwidth not available to critical business applications
- Legal issues due to staff accessing illegal websites via proxy/VPN
- Security issues due to unauthorized or malicious software installed (e.g., RAT, remote control software)
- Unintentional or malicious users expose confidential data via proxy avoidance applications

Benefits

- Eliminate use of proxy avoidance applications
- Gain back control of bandwidth management
- Restore visibility and control over user internet activity and productivity
- Prevent confidential data from leaving network
- Enforce legal compliance and Acceptable Use Policy (AUP)

Existing IAG Customer

1 Government

Pain points

- Slow Internet connectivity and unable to prioritize bandwidth for critical business applications
- Circumvention of security perimeter allows unrestricted access to unauthorized or illegal Internet activities
- Unintentional or malicious users expose confidential data via proxy avoidance applications
- Potential legal action based on illegal use or access

Benefits

- Eliminate use of proxy avoidance applications
- Gain back control of bandwidth management
- Restore visibility and control over user internet activity and productivity
- Prevent confidential data from leaving network
- Enforce legal compliance and Acceptable Use Policy (AUP)

2 Education customer

Pain points

- Constant bandwidth saturation and high cost of adding more bandwidth
- Undetected malware running through proxy avoidance applications
- Malware propagation causes network congestion and potentially bringing down the network
- Potential legal action based on illegal use or access

Benefits

- Eliminate use of proxy avoidance applications
- Better user Internet experience
- Ensuring bandwidth is only used for appropriate content
- Reducing user exposure to malware propagation with the integration of Endpoint Secure protection
- Enforce legal compliance and Acceptable Use Policy (AUP)

10. How To Sell (Guide For Region)

Regional GTM Plan

- Local solution launch
- Webinar
- Local magazine article (how many magazines should publish the article?)
- Recurring social media (weekly, monthly)
- Promotion Campaign
- Identify existing NGAF/IAG customers and follow up for upsell
- Sales & technical training to Partner
  - Plan to train partner

Channel Partners

- Government focused partner
- IAG
  -Searching for Blue Coat/SWG replacement.
  -Partner conducts customer facing meetings
  -Searching for vendors who can deliver good professional services

Channel Partners

- Education partner
- IAG
  -VAR/SI turnkey solution driven with SIA bundling.
  -Partner understands holistic solution to conduct customer health check and assessments.

11. FAQ

1. What Products Are Required For Application Containment Use Cases?

• **Proxy Avoidance** Protection requires NGAF or IAG with Endpoint Secure.

• **Whitelisting/Blacklisting** can be implemented by Endpoint Secure alone. However, better granularity selecting from running applications reported requires addition of NGAF.

Sangfor IAG non-PAP application whitelisting and blacklisting limited to domain and IP address. Current IAG Ingress agent has similar capabilities to NGAF/Endpoint Secure for blacklisting running processes, files, and registry-based rules.

• **Peripheral Control** can be implemented by Endpoint Secure alone.

Current IAG Ingress agent has similar capabilities to NGAF/Endpoint Secure for blacklisting running processes, files, and registry-based rules.

• **Network Control** requires NGAF or IAG.

Sangfor IAG has similar capabilities to NGAF/Endpoint Secure using Ingress Client to perform endpoint compliance security verification based on anti-virus software/database, login domain, operating system, access control, local windows account, etc.

2. How Many Endpoints Can Be Managed Using Application Containment?

- NGAF can manage 2000 endpoints. This will increase in a future NGAF release.
- IAG can manage 20,000 endpoints or the current limit of Endpoint Secure management.

3. How Many NGAF and IAG Can an Endpoint Be Managed By Using Application Containment?

Application Containment on an endpoint can be managed from only a single NGAF or IAG. It cannot be managed by both NGAF and IAG at the same time.

4. What Applications or Traffic Cannot Be Seen or Blocked By Application Containment?

Application Containment cannot see or block traffic controlled by web browser extensions or add-ons. That will be corrected in a future version.

5. Does Application Containment Work With Endpoint Secure Mac or Linux Agents?

Currently, Application Containment only works with Endpoint Secure Windows agents. Mac and Linux support will be available in a future version.

6. How is Application Containment licensed?

Application Containment requires Endpoint Secure Protect Ultimate Bundle agents with either minimum NGAF or IAG Essential Bundles.

7. Does Application Containment Require Additional Resources or Impact Performance on The Endpoint?

No. Application Containment does not impact system performance or system and network resources.

SANGFOR

Make IT Simpler, More Secure and Valuable !

www.sangfor.com