AlgoSec

Managing Security at the Speed of Business

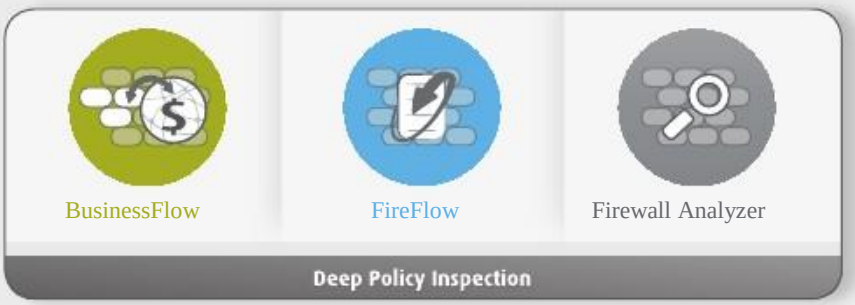
AlgoSec.com

屢獲殊榮的安全管理套件

在企業的網路保衛戰中有兩點非常關鍵，一、安全性原則的規模不斷擴大；二、多變的業務需求、分散的 IT 團隊和依靠多個互聯元件的關鍵應用程式使安全性原則的複雜程度持續加深。這使得管理防火牆策略不光需要消耗大量珍貴的資源，還容易出錯，對業務靈活性產生負面影響並且產生安全和合規鴻溝。

AlgoSec 安全管理套件為防火牆及相關安全體系結構的複雜策略管理提供自動化和以應用程式為中心的解決方案，大大提高系統安全性和業務靈活性。AlgoSec 套件彌合了安全團隊、網路和應用程式團隊之間的傳統鴻溝，從而簡化安全運行和變更管理，確保持續合規，使應用程式利用率最大化，提升服務交付速度，並提供更嚴格的安全性原則，更好地避免網路攻擊。

AlgoSec 安全管理套件的動力支援由獲得專利的 Deep Policy Inspection™ 技術提供，該技術能夠進行卓越的安全性原則分析，以更高的精確度發現更多可執行成果。



越来越多的客戶選擇信任和部署本套件

整個行業上下有分佈於 50 多個國家或地區的逾 1000 個企業依靠 AlgoSec 實現自動化安全性原則管理。無論是財富 500 強公司還是領先的服務提供者和大中型公司，這些客戶都不約而同地選擇了 AlgoSec，因為它是高超技術與力臻達成客戶成功的完美結合。

這款工具為我们承擔重任，因此工程師能夠更加專注地提供更高水平的安全性，而無需费心於進程和變更。
— Phil Packman，安全閘道操作總經理

顯而易見，“AlgoSec 志在成為合作伙伴，而不是僅僅銷售現成的產品。” — Peter Erceg，IT 安全主管

以業界內絕無僅有的退款保證作為堅強後盾

AlgoSec 致力於通過卓越的產品創新、世界一流的支持和業界絶無僅有的退款保証確保客戶完全滿意。請連上 algosec.com/satisfaction 了解更多相關訊息。

AlgoSec BusinessFlow

以應用程序為中心的安全策略管理

AlgoSec BusinessFlow 通過提供創新、以應用程式為中心的安全性原則管理確保更快提交服務並實現應用程式利用率最大化，從而彌合應用程式、安全性和操作團隊之間的鴻溝。應用程式擁有者和網路安全團隊借助 BusinessFlow 可以：

- 加快資料中心安全應用程式的服務部署、維護和安全程式解除授權
- 確定商務應用程式連接要求，並瞭解其對安全性原則的影響
- 改善對商務應用程式連接要求的可見度

將連接要求自動轉換為防火牆規則

通過自動計算對潛在防火牆規則的必要變更並觸發 AlgoSec FireFlow 中的相關變更請求，BusinessFlow 能夠快速準確地處理升級應用程式連接要求的變更。

評估網路變更對應用程式可用性的影響

BusinessFlow 說明重要的利益相關者瞭解伺服器遷移等網路變更可能會對商務應用程式產生的影響，並觸發必要的變更請求以確保應用程式可用性。

確保安全的應用程式解除授權

安全地移除已解除授權的應用程式不再需要的網路訪問，以確保在不影響其他商務應用程式的情況下加強了安全性原則。

通過中央應用程式連接門戶強化可視性

統一查看所需應用程式連線性的最新情況能夠使安全和網路團隊與商務應用程式擁有者進行更高效的溝通，加快服務提供速度。

搜索並投射潛在規則和 ACL 到應用程式

強大的搜索功能能夠將防火牆和路由器訪問規則映射到現有應用程式，大大減少填充應用程式存儲庫的時間和工作。

提供所有變更的完整審核線索

通過持續地完整記錄對同時支援內部和外部合規性授權的應用程式所作的變更，審核和合規性驗證得到簡化。

與 AlgoSec 套件緊密集成

BusinessFlow 利用 AlgoSec 防火牆分析器進行策略分析、通信類比和視覺化，以及通過 AlgoSec FireFlow 進行安全性原則變更管理。

與現有 CMDB 系统集成

BusinessFlow 利用現有 CMDB 系统中的信息簡化實施和管理。

“現在，企業網路和使用企業網路的應用程序的複雜性前所未有。清楚地了解對應用程序或服務所作的變更能夠簡化安全策略，減少進行合理活動的障礙。” – Greg Young，Gartner 研究副總裁

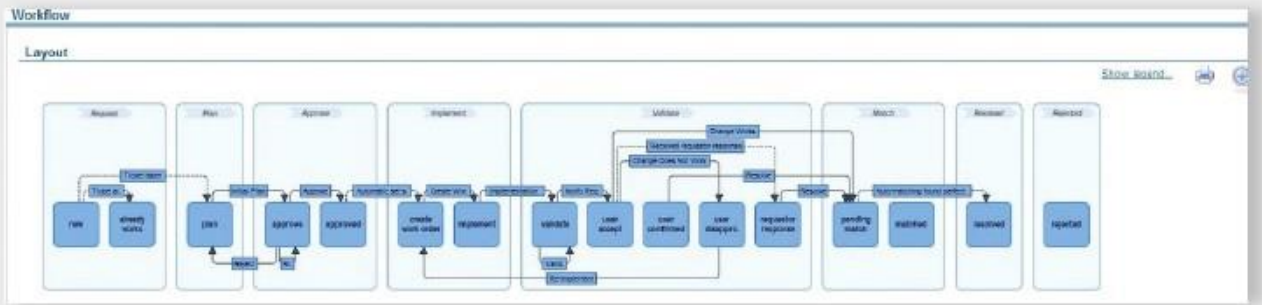
Gartner

AlgoSec FireFlow

安全性原則變更自動化

AlgoSec FireFlow 實現從提交和設計到風險分析、實施、驗證和審核這一整個安全性原則變更工作流程的自動化。FireFlow 與現有服務台票證系統無縫集成並增加了系統智慧，以便安全和操作團隊能夠：

- 減少近 60% 處理防火牆變更所需的時間
- 增強變更請求的準確性和問責性
- 強制實施合規性以及緩解不當的和進程外的變更的風險



實現安全性原則變更工作流程的自動化

FireFlow 提供添加新規則、刪除規則、變更物件和重新驗證規則的現成工作流程，使企業能夠解決更多真實狀況和提高操作效率 。

分析變更請求，確保合規性並緩解風險

FireFlow 在在每一項計畫變更被實施前自動對其進行分析，以確保其遵從法規和企業標準。FireFlow 充分利用內容極其豐富的風險知識庫，其中涵蓋了行業最佳實踐、PCI-DSS 和 SOX 等法規以及企業定義策略。

利用智慧變更管理設計排除不確定性

FireFlow 的拓撲感知演算法根據網路流量自動確認變更請求，以檢測出不必要（「已經在使用」）的變更並通知要求者，這能夠避免對高達 30% 的變更請求進行不必要的處理。FireFlow 在可執行檔詳細建議中指定了最佳安全實施，準確地描述了要添加、刪除或編輯的相關設備和規則。

節約時間，避免自動策略推送出現人工誤差

FireFlow 可以在 Check Point 防火牆上自動實施建議的策略變更，並生成 Cisco CLI 命令。

通過自動驗證和調節防止發生錯誤和未經授權的變更

FireFlow 自自動確認正確執行了變更請求，以防止過早解決票證。通過檢測實際策略變更並將其與請求票證關聯，自動匹配可防止未經授權的變更。

定制符合您獨特要求的變更工作流程

借助 FireFlow 可根據每個企業的特定要求輕鬆定制工作流程，而 FireFlow 的靈活角色和工作流程邏輯可確保問責和管理。此外，預填充範本可節約時間，並改善要求者和防火牆管理員之間的溝通效果。

跟蹤和審核整個變更週期

详詳細的報告跟蹤整個變更週期，提供 SLA 指標並大大簡化審核和合規性工作。

與變更管理系統 (CMS) 集成

FireFlow 可可與 BMC Remedy、HP Service Manager 和 CA Service Desk Manager 等現有 CMS 進行無縫集成。在 CMS 中所創建票證的狀態將不斷進行更新。

“使用 AlgoSec 後，現在我們應用防火牆變更只需以前一半的時間。並且该解決方案為我們提供的智能降低了人工誤差和風險。”
— Saul Padron，信息安全經理

Telefónica

AlgoSec Firewall Analyzer

網路安全性原則分析

AlgoSec 防火牆分析器 (AFA) 提供了對複雜安全性原則的可見度和控制能力，從而自動化防火牆運行並確保網路安全設備正確配置。安全和操作團隊借助 AFA 可以：

- 減少 80% 的防火牆審核準備時間
- 簡化防火牆操作，提高防火牆性能
- 確保更嚴謹的安全性原則，加強保護以防止網路攻擊

視覺化您的安全性原則

AFA 提供複雜網路和安全性原則的可視性，使日常防火牆操作更輕鬆、效率更高。AFA 自動生成所有網路防火牆、路由器、子網和區域的互動式拓撲圖，並可通過強大的故障排除、變更規劃和「假設」查詢即刻查看安全性原則對網路通信的影響。

監控所有網路安全性原則變更

監控並記錄網路安全性原則中的所有變更；對於未經授權或具有風險的變更，管理員將收到即時電子郵件警告。

清理和優化防火牆規則集

AFA 可以發現未使用、已覆蓋、重複和過期的規則和物件，甚至能夠整合相似規則。此外，AFA 還就如何在保持策略邏輯不變的同時重新排序規則予以明確建議，以達到最佳防火牆性能。

確保在不影響操作的情況下增強策略嚴謹度

通過自動識別過於寬泛的規則（例如任何「服務」、「應用程式」等）並根據實際使用模式進行收緊，AlgoSec Intelligent Policy Tuner™ 在不影響業務需求的情況下降低了風險。

發現具有風險的防火牆規則並緩解其風險

發現和排列防火牆策略中所有風險及其相關規則的優先順序。AFA 依據內容極其豐富的風險知識庫，其中涵蓋行業法規、最佳實踐和定制的企業策略，可確保發現更多風險。

符合基準配置，減輕網路威脅

確定基準設備配置，最大程度地減小可能會被網路罪犯利用的風險，並針對不符合基準的配置生成報告。

生成自動化審核和合規性報告

AFA 按照 PCI-DSS、SOX、FISMA 和 ISO 等企業和法規標準自動生成報告，極大地減少了審核準備工作和成本－高達 80%。AFA 可在一份報告中集合多個防火牆發現的結果，從而能夠更全面地查看一組設備的風險和合規性。

簡化防火牆遷移

AFA 通過比較不同防火牆和供應商的策略改善防火牆遷移和升級方案。此外，操作團隊可使用強大的查詢功能定位 IP 位址並確保所有連接均已就位。

> “過去每個防火牆要花上兩到三周手動完成的工作，現在只要點擊一下按鈕即可。”Marc Silver，安全經理

Discovery

規格

支持的設備

Check Point	FireWall-1®, Provider-1®, SmartCenter	v3.0 and up ,NG, NGX, Software Blade Architecture (R7x) – including Application Control and Identity Awareness
	VSX	All versions
	Security Gateway VE	All versions
Cisco	PIX, ASA Series	v4.4 and up
	Firewall Services Module (FWSM)	v1.0 and up
	Cisco Router Access Control Lists	All versions
	Cisco Layer-3 Switches	All versions
	Nexus Routers	All versions
	Cisco Security Manager	v4.3
Juniper	NetScreen Series	v5.0 and up
	Network and Security Manager (NSM)	v2008.1 and up
	SRX Series	All versions
Fortinet	Fortigate	FortOS 3.x and up, including VDOM
	FortiManager	v4.x
Palo Alto Networks	PAN-OS	v4.x and up
McAfee	Firewall Enterprise (formerly Sidewinder)	v7.x and up
Blue Coat Systems	Proxy SG	v5.x and up

支持的變更監控設備*

F5	Big-IP Family
Juniper	Secure Access SSL VPN
Linux	Netfilter/Iptables
Stonesoft	StoneGate
WatchGuard	XTM

* 可以通过 AlgoSec 扩展框架添加更多设备。

支持的變更管理系统*

BMC	Remedy
ServiceNow	Change Management
HP	Service Manager
CA	Service Desk Manager

* AlgoSec 专业服务可支持更多变更管理系统。

立即評估。申請試用 30 天的免費使用，請連結：AlgoSec.com/Eval

algosec
Managing Security at the Speed of Business

Follow Us On:

全球總部
265 Franklin Street
Boston, MA 02110

USA
+1-888-358-3696

歐洲、中東和非洲地區總部
33 Throgmorton Street

London, EC2N 2BR
United Kingdom
+44 207-156-5268

亞太地區總部
10 Anson Road, #14-06

International Plaza
Singapore 079903
+65-3158-2120