They Changed the Game

"跟著領先者走"

ForeScout 引領新一代的資訊安全趨勢

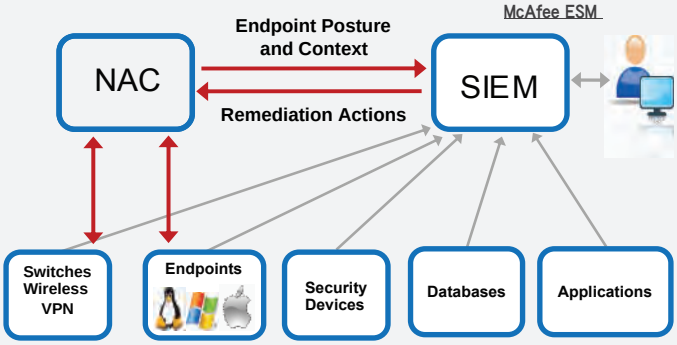
～ ControlFabric Platform = Next Generation Security ～

資安威脅會從各個環節侵入，各自獨立的IT管理很難再全面掌握有效的資訊，ForeScout推出 ControlFabric 的整合平台，將企業現有的IT環境全部連結，提供企業在管理上整合的有效資訊，帶領企業的IT管理進入新的領域。

範例: 與 SIEM 整合，雙向互動

- 攔截使用者的 web連線，通知狀況，引道自行矯正
- 將使用者導向隔離區
- 封鎖使用者的使用資源
- 封鎖 USB、應用程式等不符合公司規範的行為
- 通知使用者所招遇的情境

ArcSight
IBM QRadar
RSA enVision
Tibco LogLogic
McAfee ESM



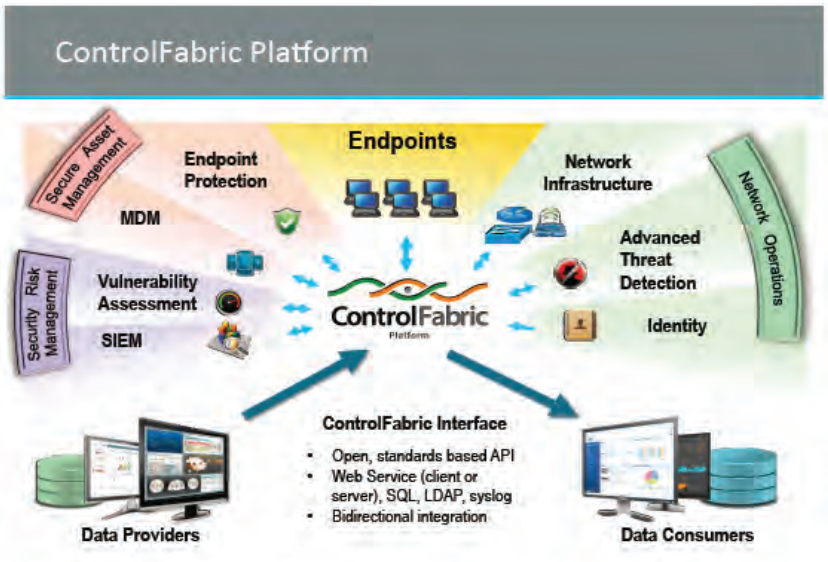
ForeScout ControlFabric SIEM Integration

ForeScout' s real-time asset intelligence expands Splunk Enterprise Analytics

ForeScout App for Splunk

ControlFabric特點：

- 改善單一環節訊息的盲點。
- 提供整合的(ForeScout與現有IT架構) 即時訊息。
- 加速矯正時間，及提供自動處理機制。
- 強化現有IT架構並簡化管理，以自動化管理系統節省大量的時間及費用。

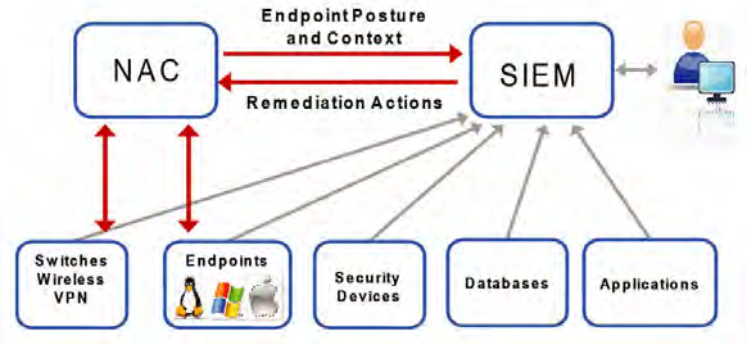


ForeScout for SIEM integration - CorreLog

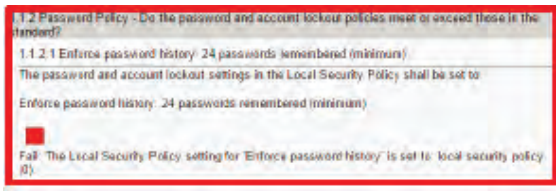
ForeScout 與 SIEM 整合 ～ 雙向互動

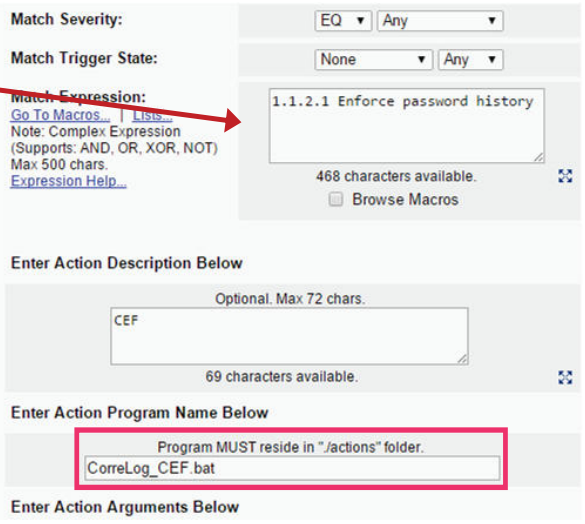
- 攔截使用者的 web連線，通知狀況，引道自行矯正
- 將使用者導向隔離區
- 封鎖使用者的使用資源
- 封鎖 USB、應用程式等不符合公司規範的行為
- 通知使用者所招遇的情境

Correlog
ArcSight
IBM QRadar
RSA enVision
Tibco LogLogic
McAfee ESM



◎ 整合範例 - 弱點掃描送syslog給Correlog，透過CorreLog Action功能去觸發 ForeScout policy進行動作。





透過3rd Party弱點掃描工具，察覺該設備目前存在Password History之漏洞，並將事件傳送至Correlog。
Correlog依據此事件定易觸發 ForeScout CounterACT NAC Policy執行控管。

Correlog 觸發 ForeScout Policy

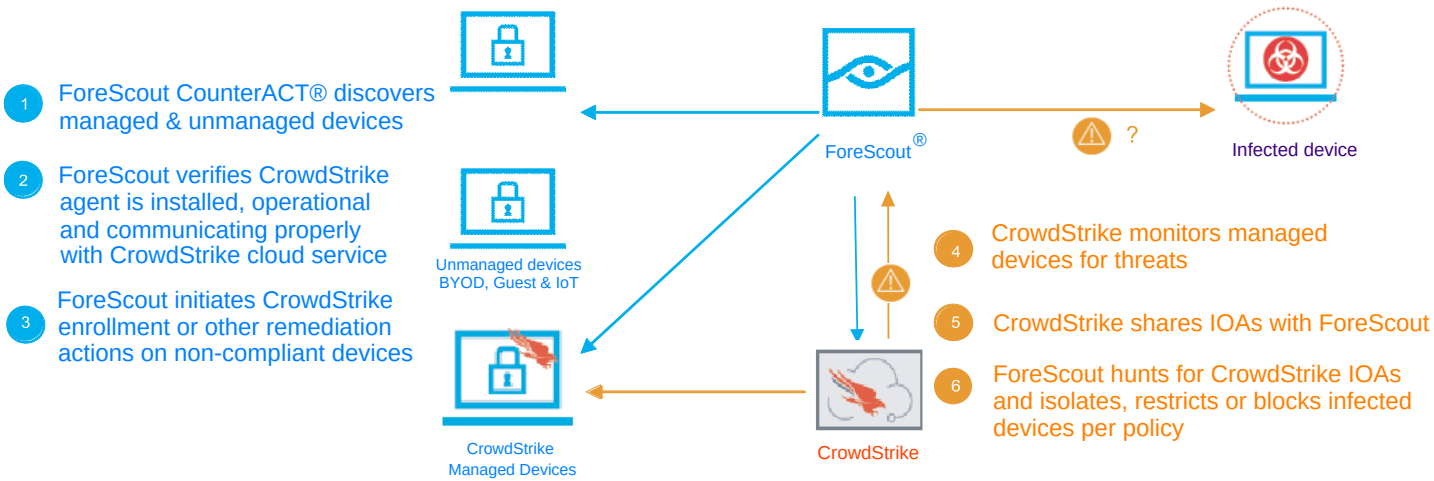
ForeScout 限制Client 網路連結

ForeScout 發表與 CrowdStrike 整合模組

用於CrowdStrike的ForeScout擴充模組可使ForeScoutCounterACT®與CrowdStrike間信息共享，並以安全的工作流程確保連網設備安全，主動檢測企業網路中的威脅並以自動化方式處置及回應，使企業得以加速資安威脅反應時效，阻擋惡意程式傳播並減少足以影響商業活動的潛在資安問題。

◆ 整合效益：

- 增加連網設備管理的可見度，提升設備管理能力。
- 縮短進階資安威脅的平均偵測及應對時間，增加企業資安防護能力。
- 可檢測CrowdStrike Agent運作狀態，增加管控範圍及深度。
- 運用ForeScout control Actions 自動回應及矯正資安事件，增進管理效率。



Brochure

ForeScout

ControlFabric™ Platform

Continous Monitoring

Security Context

Policy-based Control

Dynamic Mitigation

ForeScout

ForeScout ControlFabric Platform

Benefits

ForeScout CounterACT's native ability to provide 100% visibility and control over all endpoints on your network without the need for agents, combined with the capability to share this information with other IT management products and automate remediation from any IT management system, allows IT security managers to:

- Increase situational awareness by collapsing silos of information and leveraging real-time contextual information from ForeScout CounterACT
- Improve security posture by speeding remediation and automating response
- Maximize investment in existing network and security products by ensuring interoperability
- Advance continuous monitoring and mitigation capabilities and remove endpoint security blind spots
- Save time and money by automating routine IT tasks and processes

"ForeScout's ControlFabric platform represents a flexible approach to gain the context and policies necessary to advance endpoint compliance, continuous monitoring and security analytics."

Jon Oltsik
Senior Principle Analyst,
Enterprise Strategy Group

The Problem

If your IT security organization is like most others today, you're caught in a continuous reactionary cycle, racing to get ahead of key security issues. Over the years, you've probably purchased a variety of security and management systems to respond to rising cyber threats and the growing need to mobilize your workforce — antivirus (AV), encryption, intrusion prevention (IPS), vulnerability assessment (VA), firewalls, data leak prevention (DLP), security information and event management (SIEM) and mobile device management (MDM). Each of these systems serves a valuable function, but ask yourself two questions:

1. Is your security posture as strong as it can be?
2. Are your responses to security issues as fast and as automated as they could be?

In terms of security posture, your endpoint security systems probably rely on agents, which presumes that all endpoints are owned by your organization and are carefully managed. However, if your organization allows personally owned devices (BYOD) on your network, the inability of management systems to see and control these devices is a problem. Your endpoint management systems also can't give you visibility into non-standard or embedded systems (e.g. medical devices or industrial equipment) that do not support agents. Finally, your management systems can't deal with endpoints that have broken or misconfigured agents. Analysts report that typically 40% of endpoints in an enterprise are either invisible to traditional management systems or are out-of-compliance, weakening your security posture.

A second problem that increases security and compliance exposures is the fact that amassing a portfolio of tools to support a defense-in-depth security model inherently creates multiple silos of controls and information. Beyond sending alerts to your security management system, these silo'd tools don't communicate very effectively with one another. This robs you of critically needed synergies such as the ability to share contextual information between systems. Without information sharing, you can't optimize your IT security investments.

In terms of automation, it is likely that some of your IT security systems can't take immediate action to mitigate risk once security issues are discovered. This failure to respond quickly and automatically to violations not only costs you time and money, but it also results in persistent security issues and compliance faults, and it raises the potential for hackers to compromise your systems.

In a nutshell, your existing IT control systems may exhibit these problems:

1. Inadequate visibility of all endpoints on the network, especially BYOD
2. Lack of real-time continuous monitoring
3. Lack of coordination between security products, because they each function as a separate silo
4. Lack of automation to respond quickly to compliance violations and to contain advanced threats

While you may have previously considered this situation as either acceptable or unavoidable, many organizations are now recognizing the need for more complete visibility, more real-time assessment, and more extensive coordination and automation between IT management systems.

ControlFabric

The Solution

ForeScout ControlFabric™ helps solve the abovementioned problems. ControlFabric is an open platform that enables ForeScout CounterACT™ and other IT solutions to exchange information and more efficiently mitigate a wide variety of network, security and operational issues. As a result, you can achieve continuous monitoring and mitigation capabilities that better leverage your infrastructure investments and optimize your IT resources. By leveraging the ControlFabric partner ecosystem, you can optimize security investments, efficiently preempt and contain exposures, and enhance your overall security posture.

ControlFabric is based on ForeScout CounterACT which dynamically identifies and assesses all network users, endpoints and applications; controls network access; directly remediates endpoint security issues; and triggers 3rd party remediation systems. CounterACT natively provides real-time visibility, security posture assessment and continuous monitoring of all users and endpoints connecting to your network, including BYOD endpoints and guests. This effectively solves the visibility problems mentioned earlier.

ControlFabric extends CounterACT's capabilities and enables you to share contextual information with other security and IT management systems, thereby reducing the problem of information silos. Additionally, ControlFabric can bring real-time control and automated remediation to your IT systems that heretofore have been limited to collecting, generating, analyzing or storing information.

ControlFabric Base Integrations

ForeScout CounterACT includes a wide variety of integrations with network and IT infrastructure (switches, wireless controllers, VPN, routers, directories), endpoints (Windows, Mac, Linux, iOS, Android, printers, other devices), and endpoint software (antivirus, instant messaging, WMI, etc.). These integrations are available at no additional charge in the form of easily installed plugins. CounterACT currently supports over 60 integrations with IT infrastructure products and services. These base ControlFabric integrations give you tremendous power to discover and classify endpoints; track users and applications; assess security posture; control network access; enforce endpoint compliance policy; and fix security gaps such as broken endpoint security agents.

ControlFabric Extended Integrations

The ControlFabric partner ecosystem includes popular network, security, IT management and mobile infrastructure vendors who have teamed with ForeScout to develop ControlFabric integrations. These integrations are available as separately licensed software modules that can be added to the CounterACT appliance. Current integration modules developed and supported by ForeScout include:

- **Security Information and Event Management (SIEM)** — The ControlFabric platform helps SIEM systems obtain complete visibility of all devices on the network, not just managed devices which they are typically aware of. This allows SIEM systems to accurately assess enterprise risk. Additionally, your SIEM system can now be used as an active security control by triggering the ControlFabric platform to initiate automated remediation of the security exposure.
- **Mobile Device Management (MDM)** — The ControlFabric platform helps automate the enrollment of new mobile devices into your MDM system. Additionally, it can trigger your MDM system to re-assess the compliance of a mobile device the moment the device attempts to connect to the network, and limit or block access for unauthorized or non-compliant devices. Finally, the ControlFabric integration breaks down silos and brings MDM system information into the fold of security management systems.
- **Advanced Threat Detection (ATD)** — Your ATD products have the ability to detect advanced threats, but don't include the ability to automatically remediate the problem. Integration with the ControlFabric platform allows these products to trigger automated remediation and/or quarantine infected endpoints.
- **Vulnerability Assessment (VA)** — The ControlFabric platform can trigger your VA product to scan new devices the moment that they join the network. This provides you with more up-to-date risk information. Additionally, your VA product can trigger the ControlFabric platform to remediate, limit or block endpoints that are found to contain serious vulnerabilities.
- **McAfee ePO** — The ControlFabric platform augments your ePO deployment by bringing visibility and control over unmanaged devices, and detects and remediates missing or broken McAfee agents. ePO shares managed device compliance status with ControlFabric, which continually monitors the network and attached devices, and remediates or quarantines endpoints with security exposures.

About ForeScout

ForeScout delivers pervasive network security by allowing organizations to continuously monitor and mitigate security exposures and cyber attacks. The company's CounterACT appliance dynamically identifies and assesses all network users, endpoints and applications to provide complete visibility, intelligence and policy-based mitigation of security issues. ForeScout's open ControlFabric platform allows a broad range of IT security products and management systems to share information and automate remediation actions. Because ForeScout's solutions are easy to deploy, unobtrusive, flexible and scalable, they have been chosen by more than 1,500 enterprises and government agencies. Headquartered in Campbell, California, ForeScout offers its solutions through its network of authorized partners worldwide.

Learn more at www.forescout.com.

Availability

The ControlFabric Integration Module Early Availability is available today. It replaces the Data Exchange Module. Customers who have previously purchased a license for the Data Exchange Module and who have a valid support contract are entitled to upgrade to the the ControlFabric Integration Module.

To request a demo, visit www.forescout.com/request-demo.

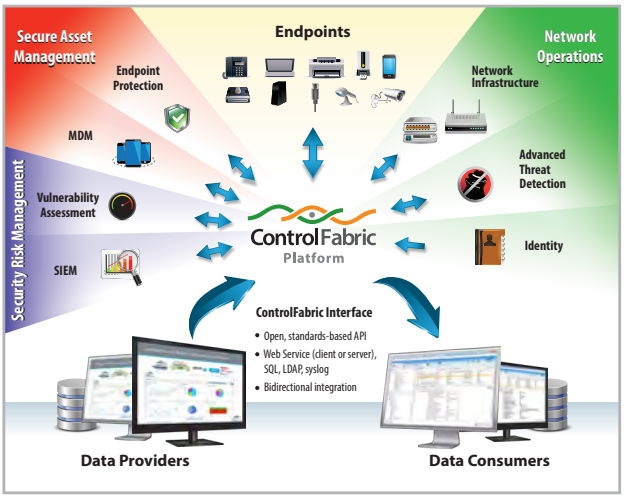


Figure 1: The ControlFabric Platform

ControlFabric Custom Integrations

ForeScout's open ControlFabric Interface allows you or any third party to easily implement new integrations based on common standards-based protocols. The ControlFabric Integration Module supports the following open, standards-based integration mechanisms:

- **Web Services API** — for sending and receiving XML messages
- **SQL** — reading from and writing to databases, e.g. Oracle, My SQL, SQL Server, etc.
- **LDAP** — reading from standard directories

Additionally, the following interface is included as a standard part of ForeScout CounterACT:

- **Syslog** — sending and receiving information via syslog

The ControlFabric Integration Module enables 3rd party products to do the following:

- ***Consume ControlFabric platform data*** such as device type, compliance status, user information, operating system information, application information, peripheral information, physical layer information, and more.
- ***Provide ControlFabric platform data*** including endpoint related properties or events that can be used within a ControlFabric platform policy.
- ***Receive or send action triggers*** that leverage intelligence provided by one 3rd party solution into a policy-based action in another 3rd party solution.

An example of how the ControlFabric Integration Module can be used is to pull and push information to/from any SQL database. Suppose you keep an asset inventory in a SQL database. ForeScout CounterACT can update the asset inventory with real-time information about everything on the network. Or, going the other way, suppose you have an inventory of company-owned iPad serial numbers or MAC addresses in a SQL database; CounterACT can query this list anytime an iPad attempts to connect to the network and apply the appropriate policy.

ForeScout

ForeScout Technologies, Inc.
900 E. Hamilton Ave.,
Suite 300
Campbell, CA 95008
U.S.A.

T 1-866-377-8771 (US)
T 1-408-213-3191 (Intl.)
F 408-213-2283
www.forescout.com

台灣區代理商
INFO SOURCE
亞太信息股份有限公司
台北市11070基隆路一段163號10F-1
TEL: 02 3765-2726 FAX: 02 3765 2730
http://www.infosoruce.com.tw

Doc: 2013.0071