



FORTINET[®]



FortiNAC -

讓你內網 IoT 無所遁形且可管理

2021

Dave Peng 彭冠嘉

Fortinet 台灣區技術顧問



Agenda



論 IoT 辨識的重要性



有了 FortiNAC, 萬事 OK



FortiNAC Demo



201705

Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

201908

微軟：俄國駭客使用IoT裝置入侵企業網路

曾經攻擊過美國民主黨、奧林匹克委員會，以VPN Filter惡意程式大規模感染路由器的國家級駭客組織APT 28，近期被發現企圖利用VoIP電話、印表機及影片解碼裝置，駭入特定企業網路

202001

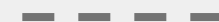
研究人員踢爆GE Medical醫療裝置含有重大安全漏洞，將允許駭客關閉監護裝置

GE Medical的醫療裝置內含6大安全漏洞，成功的開採將允許駭客關閉監護裝置、變更警報設定，或是自遠端控制相關裝置，目前GE Medical尚未完成修補作業，僅提供用戶暫時緩解方法





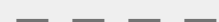
快速套用模組



弱點

跳板

不熟網路資安



不該

突破

現有產品底層



錯誤

小眾

72

裝置 & 儀器並不安全



69

裝置 & 儀器使用
應用程式並不安全

90

超過一種手持裝置

76

646 Million

IoT 設備會被採用

醫院大量使用手持裝置 / BYOD



Agenda



論 IoT 辨識的重要性



有了 FortiNAC, 萬事 OK



FortiNAC Demo

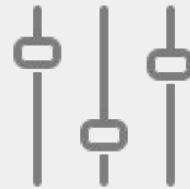


FortiNAC

看不到，則防不到



看透



控管



自動化

IoT

自動化辨識

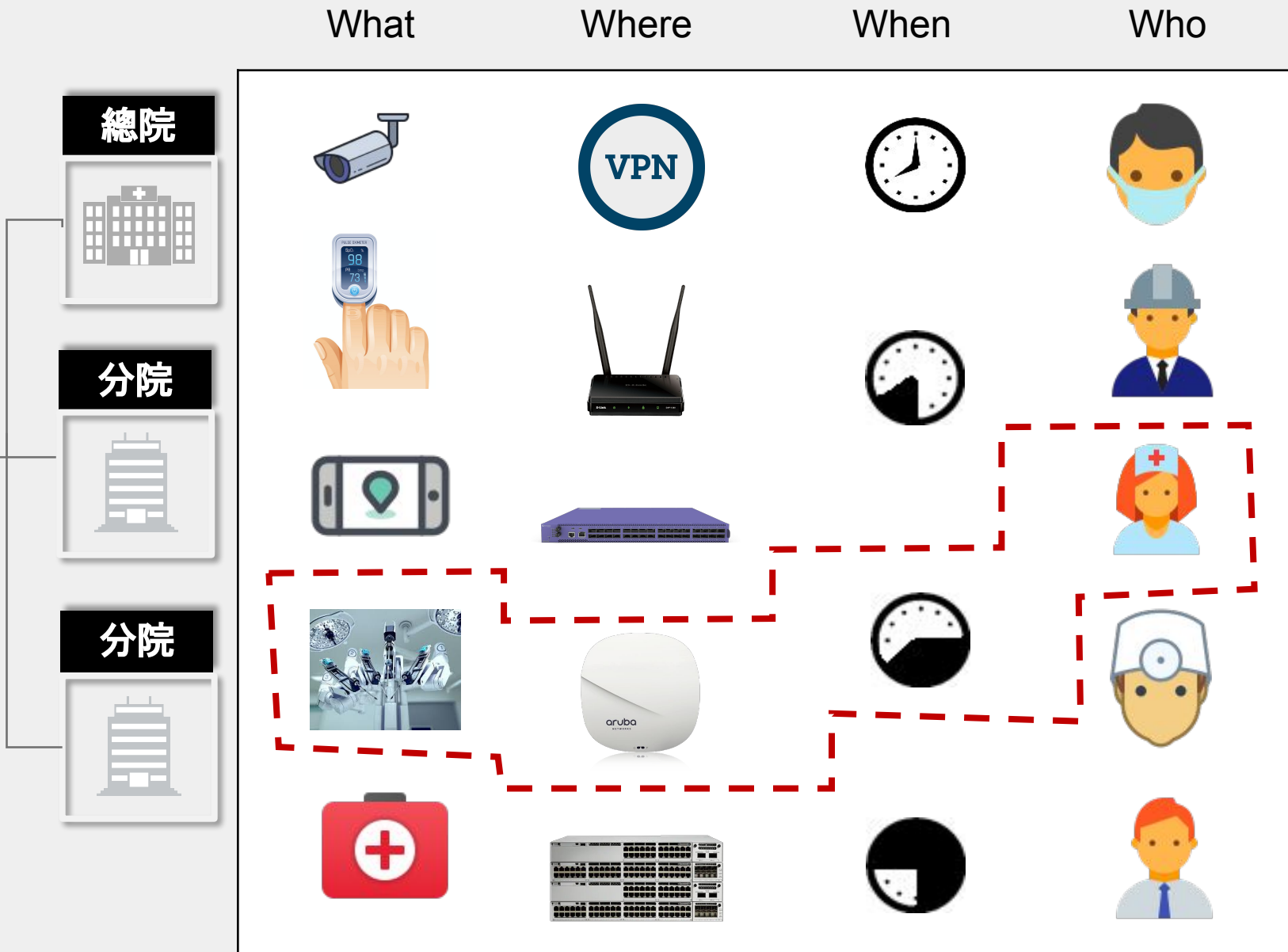
自動化辨識



NAC

零信任控管

零信任控管



先天可視性

	Samsung Electronics Co.,Ltd	58:C5:CB:69:ED:9F			WLC VLAN mmhmbtt	TT-M
	Samsung Electronics Co.,Ltd	AC:AF:B9:2E:3E:64			WLC VLAN mmhmbtt	TT-M
	GUANGDONG OPPO MOBILE TELECOMMUNICA CORP.,LTD	DC:55:83:79:18:03			WLC VLAN mmhmbtt	TT-M
	ASUSTek COMPUTER INC.	04:D4:C4:CD:F0:2E				
	ASUSTek COMPUTER INC.	04:D9:F5:F1:4E:10				
	ASUSTek COMPUTER INC.	04:D9:F5:F1:4E:69				
	ASUSTek COMPUTER INC.	04:D9:F5:F1:50:BD				
	ASUSTek COMPUTER INC.	04:D9:F5:F1:55:07				
	GUANGDONG OPPO MOBILE TELECOMMUNICA CORP.,LTD	1C:42:7D:BD:F1:B3				
	Samsung Electronics Co.,Ltd	24:5A:B5:D0:22:AF			WLC VLAN mmh-staff	TT-M
	GUANGDONG OPPO MOBILE TELECOMMUNICA CORP.,LTD	3C:F5:91:E7:39:0D			WLC VLAN mmh-staff	TT-M
	Samsung Electronics Co.,Ltd	58:C5:CB:69:F0:F9			WLC VLAN mmh-staff	TT-M
	Samsung Electronics Co.,Ltd	58:C5:CB:69:F5:E5			WLC VLAN mmh-staff	TT-M
	Samsung Electronics Co.,Ltd	58:C5:CB:69:FA:7B			WLC VLAN mmh-staff	TT-M

FortiGuard IoT Results for: DC:55:83:79:18

Category: Mobile
Subcategory: Phone
Vendor: OPPO
Model: F5
Operating System: Android
Sub Operating System:
Confidence: 37

Close

後天可視性

Modify Device Profiling Rule

General Methods

- Active
- DHCP Fingerprinting
- FortiGate
- FortiGuard
- HTTP/HTTPS
- IP Range
- Location
- Network Traffic
- ONVIF
- Passive
- Persistent Agent
- Script
- SNMP
- SSH
- TCP
- Telnet
- UDP
- Vendor OUI
- WinRM
- WMI Profile

Vendor OUI

Vendor N

Vendor N

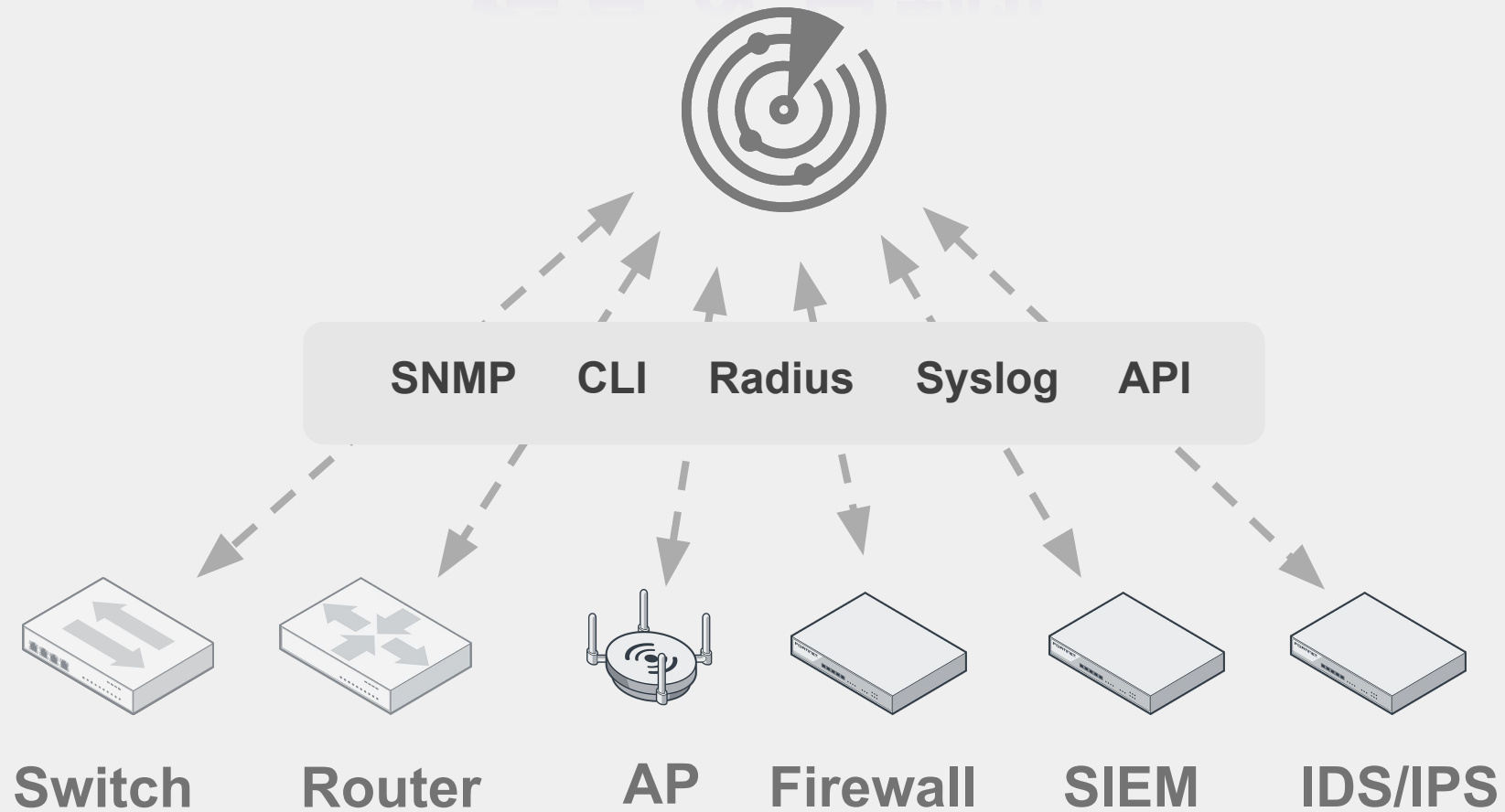
Vendor N

Vendor N

Add



控管 & 自動化





ARISTA

Support Devices



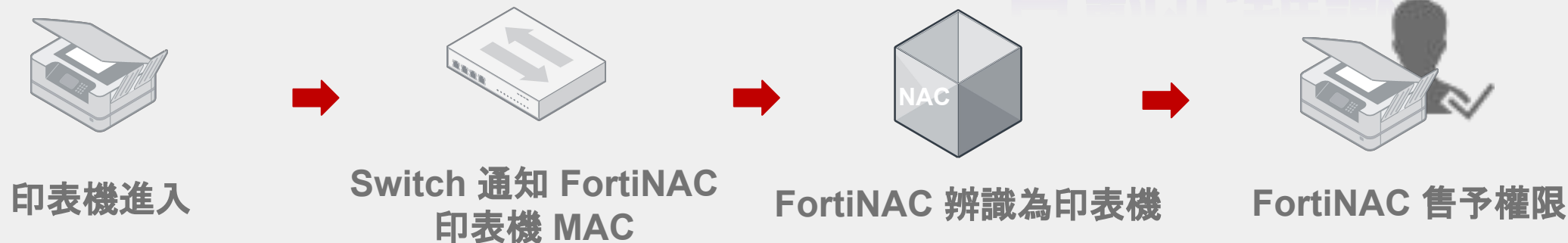
**Hewlett Packard
Enterprise**

DEVICES



FortiNAC 註冊&辨識機制

自動化辨識



FortiNAC 第一時間阻絕病毒

自動化隔離



簡單明瞭的辨識 policy

The screenshot displays the Fortinet FortiGate web interface for configuring Device Profiling Rules. The interface includes a navigation menu on the left, a top header with the URL 'fortinac.bradfordnetworks.com', and a main content area with a table of rules.

Navigation Menu:

- Dashboard
- Users & Hosts
 - Administrators
 - Guests & Contractors
 - Account Requests
 - User Accounts
 - Hosts
 - Adapters
 - Applications
- Locate
- Manage Hosts and Ports
- Scan Results
- Send Message
- Fortigate Sessions
- Device Profiler
- Device Identity
- Profiled Devices**
- Settings

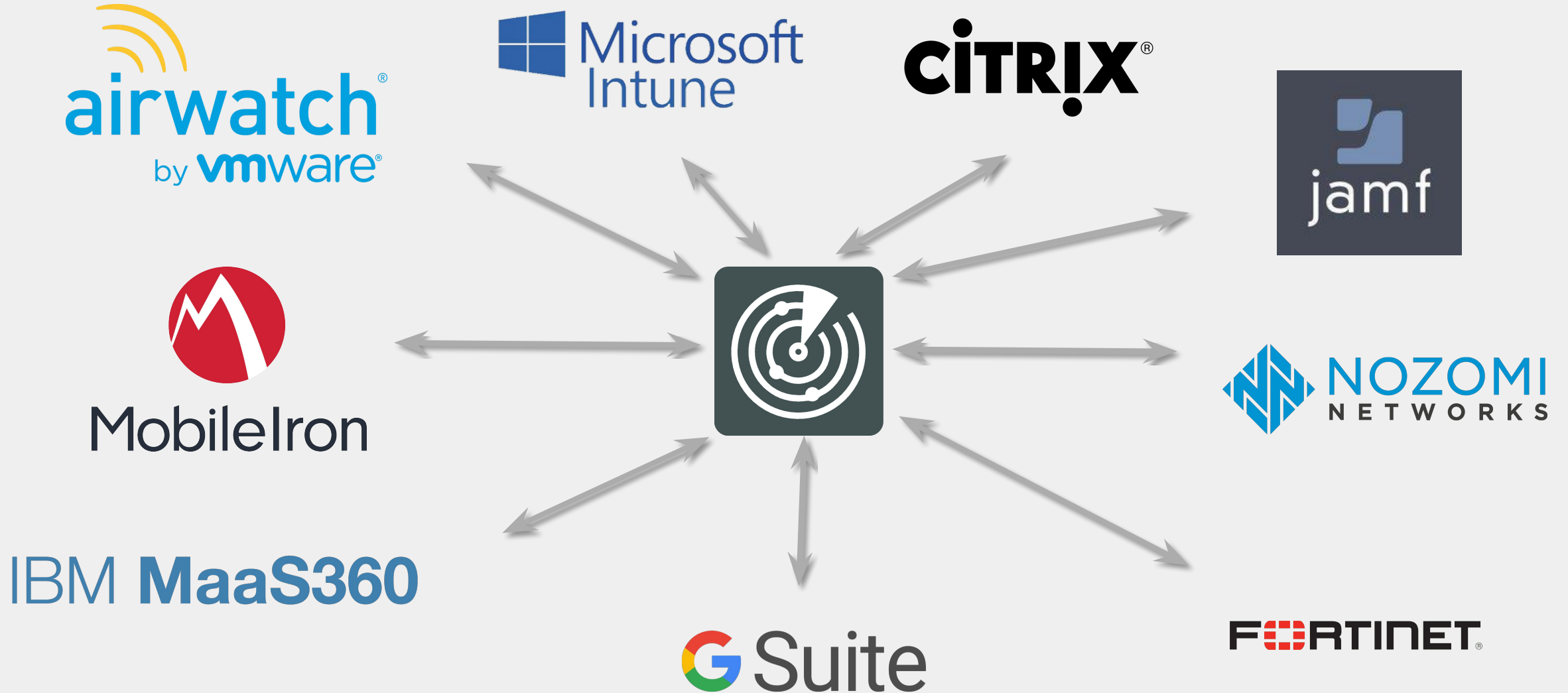
Device Profiling Rules - Total: 18

Rank: [Up] [Down] [Set Rank] Enable: [On] [Off] Rogue Evaluation Queue Size: 0 [Detail] [Flush]

Enabled	Rank	Name	Type	Registration	Methods	Register as Device	Confirm Rule On Connect
<input type="checkbox"/>	1	Android (DHCP)	Android	Automatic	DHCP	Host View	<input type="checkbox"/>
<input type="checkbox"/>	2	Apple iOS (DHCP)	Apple iOS	Automatic	DHCP	Host View	<input type="checkbox"/>
<input type="checkbox"/>	3	Mobile Device (DHCP)	Mobile Device	Manual	DHCP	Host View	<input type="checkbox"/>
<input type="checkbox"/>	4	Windows (DHCP)	Windows	Manual	DHCP	Host View	<input type="checkbox"/>
<input type="checkbox"/>	5	Linux (DHCP)	Linux	Manual	DHCP	Host View	<input type="checkbox"/>
<input type="checkbox"/>	6	Unix (DHCP)	Unix	Manual	DHCP	Host View	<input type="checkbox"/>
<input type="checkbox"/>	7	Printer (DHCP)	Printer	Manual	DHCP	Host View	<input type="checkbox"/>
<input type="checkbox"/>	8	Printer (TCP:80,515,9100)	Printer	Manual	TCP	Host View	<input type="checkbox"/>
<input type="checkbox"/>	9	IP Phone (DHCP)	IP Phone	Manual	DHCP	Host View	<input type="checkbox"/>
<input type="checkbox"/>	10	Gaming (DHCP)	Gaming Device	Manual	DHCP	Host View	<input type="checkbox"/>
<input type="checkbox"/>	11	Apple iPhone (TCP:62078)	Mobile Device	Manual	TCP	Host View	<input type="checkbox"/>
<input type="checkbox"/>	12	Mac OS X (DHCP)	Mac OS X	Manual	DHCP	Host View	<input type="checkbox"/>
<input checked="" type="checkbox"/>	13	script	Point of Sale	Manual	Script	Host View	<input type="checkbox"/>
<input checked="" type="checkbox"/>	14	fortiguard - type	Windows	Manual	FortiGuard	Host View	<input type="checkbox"/>
<input checked="" type="checkbox"/>	15	fortiguard - windows	Windows	Manual	FortiGuard	Host View	<input type="checkbox"/>
<input checked="" type="checkbox"/>	16	fortiguard - printer	Printer	Manual	FortiGuard	Host View	<input type="checkbox"/>
<input checked="" type="checkbox"/>	17	fortiguard - nas	NAS	Manual	FortiGuard	Host View	<input type="checkbox"/>
<input type="checkbox"/>	18	Catch All		Manual			<input type="checkbox"/>



FortiNAC Connector



FortiNAC Connector

qa6-145:9.0:FortiNAC-VM-CA X +

https://192.168.6.145:8443/gui/network/service-connectors/new

qa6-145.bradfordnetworks.com

root

Create Service Connector

Authentication Sources

Google Auth RADIUS

MDM Servers

Air Watch Fortinet EMS Google GSuite JAMF MaaS360 Microsoft InTune Mobile Iron Nozomi XenMobile

Return

Dashboard >

Users & Hosts >

Network >

Inventory ☆

Logical Networks ☆

Service Connectors ☆

CLI Configuration ☆

L2 Polling ☆

L3 Polling ☆

Connections ☆

Port Changes ☆

Settings ☆

Policy & Objects >

Security Configuration >

Portal Configuration >

Logs >

System >



FortiNAC Connector - JAMF

The screenshot displays the FortiNAC web interface. The left sidebar contains navigation options: Dashboard, Users & Hosts (Administrators, Guests & Contractors, Account Requests, User Accounts, Hosts, Adapters, Applications, Locate, Manage Hosts and Ports, Scan Results, Send Message, Fortigate Sessions), Device Profiler (Device Identity, Profiled Devices), Settings, Network, and Policy & Objects. The main content area shows a list of hosts under the 'Hosts' section. A modal window titled 'Applications' is open, displaying a table of security applications for a selected host. The table includes columns for Threat Score, Name, Version, Vendor, and Operating System. A 'Set Threat Override' button is visible at the top of the modal. The 'Hosts' list shows various devices including iPads and iPhones with their respective status icons.

Hosts - Displayed: 50 Total: 42

Applications

Set Threat Override

Export to: CSV PDF RTF

Security Applications - Total: 66

Threat Score	Name	Version	Vendor	Operating System	Opera
	Sports Illustrated	7.17		iOS iPad	iPa ^
	TED	2267		iOS iPad	iPa
	The Economist	2.13.1		iOS iPad	iPa
	Thermostat	726		iOS iPad	iPa
	Tiger 12	1.0.8		iOS iPad	iPa
	TripAdvisor	248		iOS iPad	iPa
	Twitter	6.15.1		iOS iPad	iPa
	VLC	2.3.0		iOS iPad	iPa
	Weather+	2.50		iOS iPad	iPa
	WebMD	11247		iOS iPad	iPa
	YouTube	2.13.11403		iOS iPad	iPa
	Zillow	8.1.6407		iOS iPad	iPa v

Close



Agenda



論 IoT 辨識的重要性



有了 FortiNAC, 萬事 OK

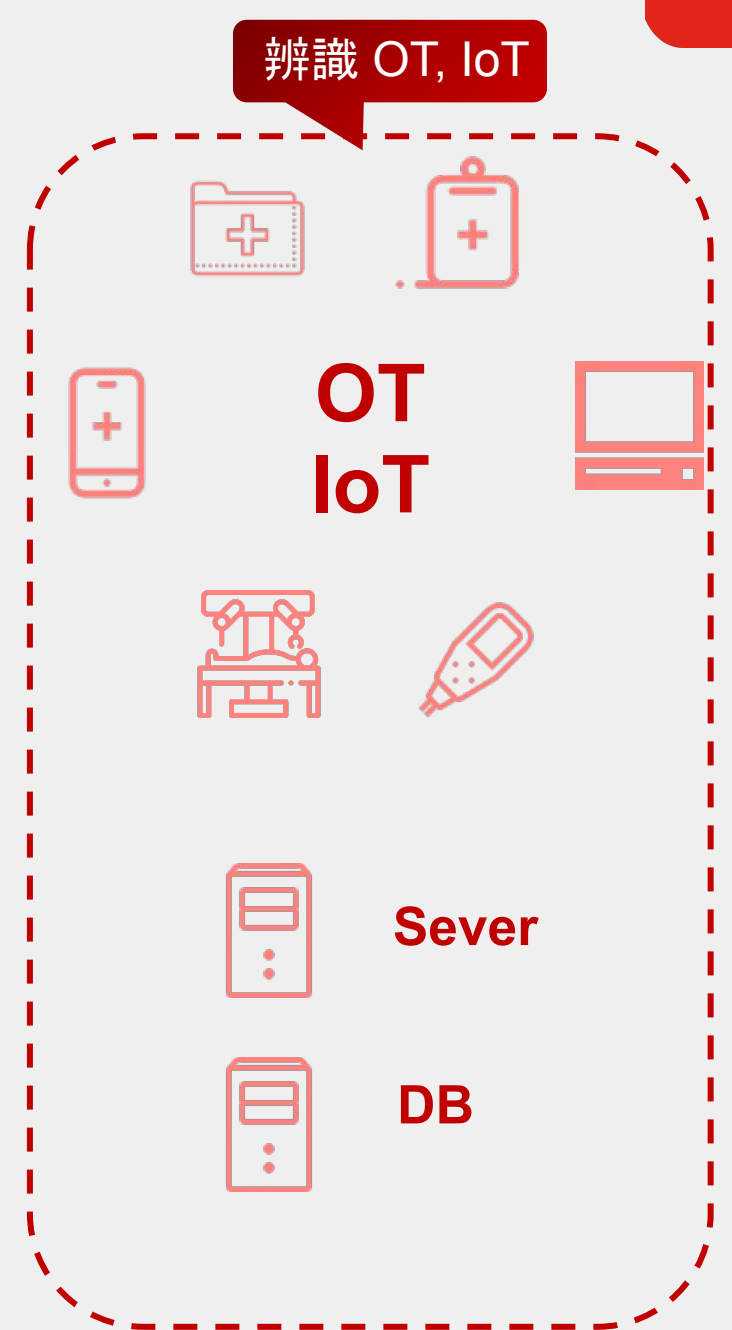
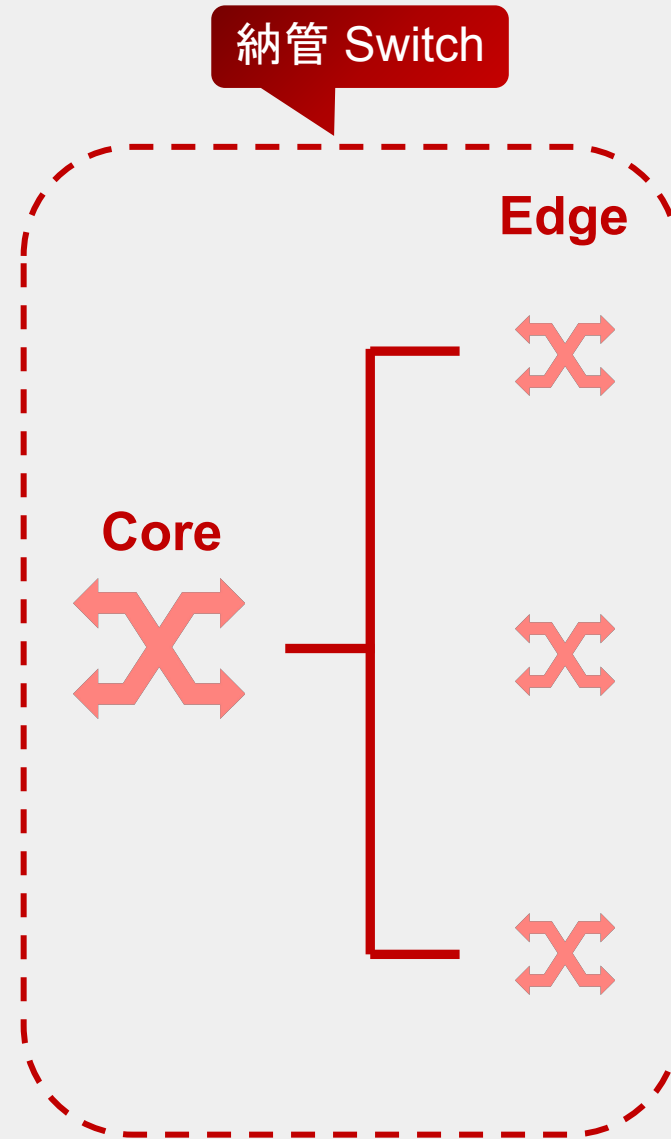


FortiNAC Demo



架構

FortiNAC



MIC 設備



Status	Vendor Name	Physical Address	Host Status	Location	Connected Container	Rule Name	Access Value	Operating System	Host Created	Host Last Connected
	HUAWEI TECHNOLOGIES CO.,LTD	24:31:54:F8:7C:52		WLC VLAN ncjs-ap	TT-MMH		ncjs-ap	Android Tablet Android	12/23/20 10:26 AM GMT+0800	01/18/21 01:13 PM GMT+0800
	HUAWEI TECHNOLOGIES CO.,LTD	F4:63:1F:CD:3C:17		WLC VLAN mmh-guest	TT-MMH	FortiGuard-Android	mmh-guest	Android Phone Android	12/24/20 09:58 AM GMT+0800	01/18/21 09:49 AM GMT+0800
	HUAWEI TECHNOLOGIES CO.,LTD	F4:BF:80:B7:5B:17		WLC VLAN mmh-staff	TT-MMH		mmh-staff		01/18/21 03:35 PM GMT+0800	01/18/21 04:26 PM GMT+0800



Status	Vendor Name	Physical Address	Host Status	Location	Connected Container	Rule Name	Access Value	Operating System	Host Created	Host Last Connected
	Xiaomi Communications Co Ltd	20:47:DA:2A:C6:97		WLC VLAN mmh-guest	TT-MMH	FortiGuard-Android	mmh-guest	Android Phone Android	01/02/21 08:02 PM GMT+0800	01/18/21 04:56 PM GMT+0800
	Xiaomi Communications Co Ltd	EC:D0:9F:38:B4:0A		WLC VLAN mmh-guest	TT-MMH	FortiGuard-Android	mmh-guest	Android Phone Android	12/25/20 09:43 AM GMT+0800	01/18/21 04:46 PM GMT+0800
	Xiaomi Communications Co Ltd	F4:F5:DB:CB:0B:E7		WLC VLAN mmh-guest	TT-MMH		mmh-guest		01/17/21 03:11 PM GMT+0800	01/17/21 03:31 PM GMT+0800



Status	Vendor Name	Physical Address	Host Status	Location	Connected Container	Rule Name	Access Value	Operating System	Host Created	Host Last Connected	Host Inactivity Date
	Shenzhen TINNO Mobile Technology Corp.	B4:39:39:18:15:37		WLC VLAN mmh-staff	TT-MMH		mmh-staff	Android Phone Android	12/21/20 05:56 PM GMT+0800	01/04/21 08:50 PM GMT+0800	01/18/21 08:50 PM GMT+0800
	Shenzhen TINNO Mobile Technology Corp.	BC:41:01:F7:37:23		WLC VLAN mmh-guest	TT-MMH	FortiGuard-Android	mmh-guest	Android Phone Android	12/24/20 09:57 AM GMT+0800	01/16/21 03:48 PM GMT+0800	
	Shenzhen TINNO Mobile Technology Corp.	44:D3:AD:D8:F0:DD		WLC VLAN mmh-guest	TT-MMH	FortiGuard-Android	mmh-guest	Android Phone Android	12/25/20 08:01 AM GMT+0800	12/25/20 02:27 PM GMT+0800	



MIC 設備



Status	Vendor Name	Physical Address	Host Status	Location	Connected Container	Rule Name	Access Value	Operating System	Host Created	Host Last Connected	Host Inactivity Date
	Shanghai Huaqin Telecom Technology Co.,Ltd	90:21:81:F6:30:5B		WLC VLAN mmh-staff	TT-MMH		mmh-staff		12/29/20 05:14 PM GMT+0800	01/11/21 05:32 PM GMT+0800	01/25/21 05:32 PM GMT+0800

Status	Vendor Name	Physical Address	Host Status	Location	Connected Container	Rule Name	Access Value	Operating System	Host Created	Host Last Connected
	Hangzhou Hikvision Digital Technology Co.,Ltd.	28:57:BE:84:F4:CB		A-ft-5f-c2960-1-50 Gi0/18 (DVR_IDF)	TT-MMH		10	Network NAS	12/21/20 05:16 PM GMT+0800	12/21/20 05:16 PM GMT+0800

Status	Vendor Name	Physical Address	Host Status	Location	Connected Container	Rule Name	Access Value	Operating System	Host Created	Host Last Connected	Host Inactivity Date
	Shenzhen Geniatech Inc, Ltd	AC:DB:DA:52:C7:AF		A-ft-2f-c2960-2-24 Gi2/0/34 (A2322)	TT-MMH	FortiGuard-Mobile-Device-2	226	Mobile Device Android Phone Android	12/21/20 05:38 PM GMT+0800	01/05/21 11:15 AM GMT+0800	
	Shenzhen Geniatech Inc, Ltd	AC:DB:DA:54:6D:A8		A-ft-2f-c2960-2-24 Gi2/0/35 (A2323)	TT-MMH		226	Cable Box Android	12/22/20 09:19 AM GMT+0800	01/18/21 04:08 PM GMT+0800	02/01/21 04:08 PM GMT+0800

Status	Vendor Name	Physical Address	Host Status	Location	Connected Container	Rule Name	Access Value	Operating System	Host Created	Host Last Connected
	Shanghai TYD Electronic Technology Co. Ltd	C8:AE:9C:D4:81:8B		WLC VLAN mmh-staff	TT-MMH	FortiGuard-Android	mmh-staff	Android Phone Android	12/29/20 09:57 AM GMT+0800	01/18/21 05:27 PM GMT+0800
	Shanghai TYD Electronic Technology Co. Ltd	C8:AE:9C:D4:F3:3C		WLC VLAN mmh-guest	TT-MMH		mmh-guest		01/13/21 02:26 PM GMT+0800	01/13/21 07:31 PM GMT+0800

<< first < prev 1 next > last >> 100

Status	Vendor Name	Physical Address	Host Status	Location	Connected Container	Rule Name	Access Value	Operating System	Host Created	Host Last Connected
	Zhejiang Dahua Technology Co., Ltd.	90:02:A9:B0:E0:BB		B-ft-b1f-c2960-1-10 Gi1/0/14	TT-MMH	FortiGuard-IPCam	10	Camera IP Camera	12/21/20 05:28 PM GMT+0800	01/07/21 06:26 PM GMT+0800
	Zhejiang Dahua Technology Co., Ltd.	90:02:A9:B0:E0:B6		B-ft-5f-c2960-1-5 Gi1/0/10	TT-MMH	FortiGuard-IPCam	10	Camera IP Camera	12/21/20 05:28 PM GMT+0800	12/21/20 05:18 PM GMT+0800

上海天奕达电子科技有限公司

上海天奕达 (TYD) 电子科技有限公司是一家集研发、设计、服务为一体的现代化高新技术企业，专业从事智能手持、智能穿戴、物联网IoT等产品的开发与服务。



自動化辨識 & 管理

The screenshot displays the FortiNAC-VM-Control and Application Server dashboard. The interface includes a navigation menu with options like Bookmarks, Users, Hosts, Network Devices, Logs, Policy, System, and Help. The main content area is divided into several summary panels:

- Summary:** Provides basic system information for FortiNAC-Control and Application Server, including Host Name (fnac.fortiad.info), Status (Running), Product, Version (8.3), Appliance (VM-NS500CA), and Firmware (6.3.0.79).
- Network Device Summary:** A table showing the status of network devices. It includes columns for Device, Total, Operating, and Error counts.
- Host Summary:** A table showing the status of hosts, categorized by Type, Total, Online Enabled, Offline Enabled, Online Disabled, and Offline Disabled.
- Alarms:** A section for managing alarms, including a table of latest alarms and options for filtering and acknowledging them.
- Scans:** A section for managing scans, including a chart showing Scans Per Day and options for filtering and refreshing the data.
- User Summary:** A table showing the status of users, including Type, Total, Enabled, and Disabled counts.
- License Information:** A table showing the status of licenses, including Type, Total, In Use, Available, and % Used.
- Persistent Agent Summary:** A table showing the status of persistent agents, including Version, Total, Windows, Mac-OS-X, and Linux (x86_64) counts.

S108DVU-84Y8N

Portname

- port1
- port2
- port3
- port4
- port5
- port6
- port7
- port8
- internal

Flags: QS(8

TS(static t

MI(mirror i

S108DVU-84Y8N



非資產之隔離



The screenshot displays the FortiNAC-VM-Control and Application Server dashboard. The interface includes a navigation menu with options like Bookmarks, Users, Hosts, Network Devices, Logs, Policy, System, and Help. The main content area is divided into several summary and data panels:

- Summary:** Provides details for the FortiNAC-Control and Application Server, including Host Name (fnac.fortiad.info), Status (Running), Product, Version (8.3), Appliance (VM-NS500CA), and Firmware (6.3.0.79).
- Network Device Summary:** A table showing the status of various network devices.
- Host Summary:** A table detailing the status of registered and unregistered hosts.
- Alarms:** A table listing the latest security risk alarms, all categorized as 'Security Risk Host' for 'nac-client'.
- Scans:** A section with a 'Scans Per Day' chart and a table for scan results.
- User Summary:** A table showing user registration statistics.
- License Information:** A table showing the status of concurrent licenses.
- Persistent Agent Summary:** A table showing the status of persistent agents across different operating systems.

Property	Value
Host Name	fnac.fortiad.info
Status	Running
Product	FortiNAC-Control and Application Server
Version	8.3
Appliance	VM-NS500CA
Firmware	6.3.0.79

Device	Total	Operating	Error
Server	1	1	0
Switch	1	1	0
Wireless Access Point	1	1	0
Ports	14	14	0

Type	Total	Online Enabled	Offline Enabled	Online Disabled	Offline Disabled
Registered Hosts (total)	1	0	1	0	0
- Safe&Authenticated	1	0	1	0	0
- At Risk	0	0	0	0	0
- Pending at Risk	0	0	0	0	0
- Not Authenticated	0	0	0	0	0
- At Risk&Not Auth	0	0	0	0	0
- Pending Risk&Not Auth	0	0	0	0	0
Unregistered Hosts	1	0	1	0	0
IP Phones	0	0	0	0	0
Total	2	0	2	0	0

Date	Alarm	Element
01/10/19 12:28 AM GMT+0000	Security Risk Host	nac-client
01/10/19 12:15 AM GMT+0000	Security Risk Host	nac-client
01/10/19 12:15 AM GMT+0000	Security Risk Host	nac-client
01/10/19 12:15 AM GMT+0000	Security Risk Host	nac-client
01/10/19 12:15 AM GMT+0000	Security Risk Host	nac-client

Chart	Start Day	End Day
Scans Per Day	12/19/2018	1/11/2019

Type	Total	Enabled	Disabled
User Registrations	1	1	0

Type	Total	In Use	Available	% Used
Concurrent Licenses	250	1	249	0%

Version	Total	Windows	Mac-OS-X	Linux (x86_64)

FORTINET®