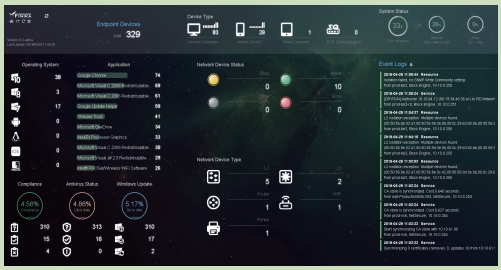
FINIKA

A Joint Information Security Defense Platform

Comprehensive Network Access Control (NAC)
Visibility and Management of IoT



Dashboard

Highlights

- Distributed/Centralized Architecture
- Wired/Wireless Management
- Endpoint Device Pre-check
- Non-Agent Based
- Support of Cross-brand Devices
- Database Integration
- Overview Dashboard
- Support of 802.1x
- Network Device Monitoring
- Compliance Check
- User-tailored Reporting System
- Multi-language Interface

Challenges of Information Security

With the continuous innovations in Technology, the use of cloud services, artificial intelligence (AI) and Internet of Things (IoT) not only drastically changes our lifestyle but also challenges existing business application services. The recent enterprise/government hacking incidents as well as the newly announced IoT regulation make the issue of security long swept under the carpet come to the fore. What can be done to get the security defense achieved?

Finika offers a Joint Information Security Defense

Through Finika, the collected data can be correlated with the back-end big data platform, and the IoT device can be automatically identified and categorized, according to the device characteristics. The overview dashboard provides a real time summary of all connected devices in the environment, illegal devices found are blocked to deny the network access, and built-in 50+ management policies can be tailored to line up with the corporate's information security principles and practices. Finika can integrate with a variety of third-party systems, such as WSUS, anti-virus system, asset system and etc. Via a single platform, Finika significantly reduces information assets management workloads by displaying and analyzing statistics gathered from different systems on a single page, and effectively achieves a joint information security defense with its flexible policy designs and user-tailored reporting system to realize the information security management and requirements.

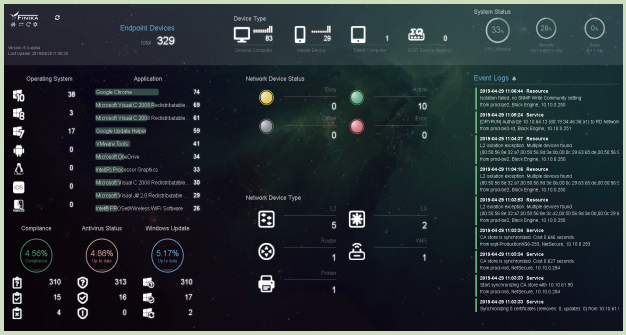
EQ Information Technologies, Inc.
Tel: (02)7716-8868 Fex: (02)2999-8440 Mail: sales@eqit.com.tw www.eqit.com.tw

FINIKA

資訊安全聯合防禦平台

全方位的網路存取控制(NAC)解決方案

高可視化的物聯網(IoT)設備管理



Dashboard

產品亮點

- 分散式/集中式架構
- 支援有線/無線納管
- 端點設備預先檢查
- 無須安裝代理程式
- 支援多家廠牌設備
- 資料庫整合
- 全方位儀錶板
- 支援802.1x
- 網路設備監控
- 合規檢查
- 自定義報表
- 支援多國語系

資訊安全所面臨的挑戰

科技不斷的創新，現今的雲端服務(Cloud)、人工智慧(AI) 及物聯網(IoT) 的運用，不僅劇烈改變我們的生活模式，也挑戰著既有的商業應用服務。

科技的進步提升了企業服務的水平，但其中資安問題也不斷的浮上檯面，企業/政府中毒事件以及2018年政府IoT政策，讓大眾對於資安問題日漸重視，但怎麼做才可以做到完整的資安防禦?

利用Finika達到資訊安全聯合防禦

透過Finika主動/被動蒐集資訊，可將蒐集來的資訊依照裝置特徵與後端大數據平台進行關聯分析，進而自動識別IoT裝置類別。

管理者可透過數據中心監控儀表板，快速掌握企業內部所有連網設備之資訊，內建50+管理政策可依據企業內部規範進行彈性化調整，並可透過網路存取控制(NAC)直接對違規設備進行封鎖。

可與多種第三方系統 (ex: WSUS、防毒系統、資產系統...)進行整合，在單一平台上統合多套系統之資訊，以達到資訊安全聯合防禦，並大幅減少管理者之工作量。

一休資訊科技股份有限公司

Tel: (02)7716-8868 Fex: (02)2999-8440 Mail: sales@eqit.com.tw www.eqit.com.tw