Mancala Networks background

- Privately owned French SAS
- Headquarters: Grenoble, France
- Mission: Develop innovative network monitoring & control solutions for Enterprises & Managed Security Service Providers (MSSPs)
- Seasoned Executive & Technical team
- Experience developing mission critical systems: SITA, Thales, BT roaming platform (CSL), …
Agenda

- Mancala Networks
- The challenge
- Solution: Network Controller
- Architecture
- Demonstration
The modern enterprise network is a complex jungle.
Mancala Networks develops software solutions that boost the security of enterprise networks

The **Mancala Network Controller** provides continuous network monitoring and control to protect the enterprise against unseen threats.

Real-time visibility and control delivers:

- A more robust, more secure corporate network
- Continuous compliance with security policies aligned with your business objectives
80% of attacks with financial impact come from the internal network

Computer Security Institute, 2011
Focus has been on protecting the network from the outside
Leaving the inside either locked or poorly controlled

Today’s ongoing revolutions exacerbate the problem

Enterprises must take back control over their networks!

- 15% to 25% of devices are not managed
  - Sophos, IDC, 2011

- By 2015, the number of connected devices will be 15 billion
  - Cisco VNI Forecast 2011

- 95% of information workers use at least one self-purchased device at work
  - IDC, 2011
A large gap exists between the perceived and actual security state of the network

Threats are obscured by a rapidly changing, complex environment.

- 15 - 25% of devices on an enterprise network operate without an organization’s knowledge, unknown to network and security managers.

- Management and security measures are applied irregularly

You can’t secure what you can’t see!
Contextual network visibility is key

### Rogue network equipment
- **Error**: detect_duplicate_ip
- **Warning**: detect_unauthorized_access_point_by_mac
- **Critical**: detect_unauthorized_dhcp_server_by_service
- **Error**: request_dot1x_auth_before_dhcp
- **Warning**: request_mac_auth_before_dhcp
- **Warning**: detect_unauthorized_router_by_mac

### Unauthorized endpoints
- **Status**: Active (online)
- **Hostname**: desk-7
- **Operating System**: Windows XP
- **Type**: PC

### Misconfigured network equipment
- **Status**: Active (online)
- **Hostname**: Cisco_AIR-1120B
- **Operating System**: iOS 12.3(9)E
- **Type**: WAP

### Malfunctioning endpoint agents
- **Status**: Active (online)
- **Hostname**: unknown
- **Operating System**: unknown
- **Type**: unknown
PwnPlug (http://www.pwnieexpress.com)
- Wireless, wired, 3G interfaces
- Automatic 802.1X and NAC bypass functionality
- Out of band SSH access over 3G/GSM
- 16 GB storage
- Tunnels through application aware firewalls & IPS
- Unpingable & no listening ports in in stealth mode
- Preloaded with Ubuntu, Metasploit, SET, Fasttrack, SSLStrip, nmap, dnsniff, netcat, nikto, nbtscan, scapy, ettercap, JRE, Medusa, …

The Network Controller could! *
Agenda

1. Mancala Networks
2. The challenge
3. Solution: Network Controller
4. Architecture
5. Demonstration
Network Controller

by mancala networks

Continuous network monitoring and control
real time, easy to deploy, modular, scalable
Optimizing the security investments of enterprise networks of any size
Mancala Network Controller

Boosts the security and manageability of IP networks for Enterprises and Managed Service Providers

- Complete network visibility including devices, users & locations
- Real-time security for all device categories, including mobile devices & BYOD
- Built-in service automation platform for IT organization and MSSP operational efficiency

4/11/12

© 2009-2012 Mancala Networks
Single solution
Multi-source network Scanner
Next-generation, context-aware NAC
Device aware IDS/IPS

- Pluggable with existing network Infrastructure and Services
- Orchestrated by a powerful Policy Engine

Internet

DNS  DHCP  AAA  SIP

Patent pending EP 10306073.7, USA 13/240,299
Optimize existing tools

> Ensure 100% BYOD enrollment
Harden MDM deployments by eliminating unknown devices in order to maximize your MDM investment

> Optimize SIEM
Provide additional log information regarding network context changes for evaluation & create real-time enforcement policies easily

> Create a “Golden” CMDB
Make sure that your asset management tools truly reflect the reality of your network infrastructure and eliminate rogue devices.

> Target vulnerability assessment
Evolve from a periodic, ineffective and reporting centric assessment strategy toward targeted, real-time assessment

Optimize existing security investments
Architecture

EP N°10306073.7
USA 13/240,299

Services

Events

Actions

Policy engine

Data model

Rules

Real-time Inventory

Configured

Actual

API

CLI

Web GUI

Configure

Report

Configure

Actual

Real-time Inventory

Export

Import

Storage & interfaces

Replication

ODBC

Files

LDAP

Services

...
The Network Controller approach:

Simplify Migration Process

- Open Network
- MAC Auth Network

Learn devices → MAC Auth
Auto Migrate ACL → 802.1X

Give visibility on non migrated devices

Fine granularity for migration (up to switch port)

Administer once migrated
Without the Network Controller:

- Configure the switch port for 802.1X access
- The device(s) can no longer connect :(
- Configure the device(s) to perform 802.1X
- Repeat for each port... :(

A common strategy: Migrate all port and devices over a WE... Good luck!
Without the Network Controller:

A smarter alternative:

- Configure the switch port for 802.1X access and Mac Auth for the devices connected to that port.
- The device can still connect (better!)
- Configure the device(s) to perform 802.1X
- Remove Mac Auth for the device(s)
- Repeat for each port... :(

What if device was mis-configured?

- Device Can no longer connect :(
Mancala Networks

The challenge

Solution: Network Controller

Architecture

Demonstration
**Functionality**

**INTERFACES**
- Interface d’administration extensible et documentée (CLI)
- Interface graphique intuitive et unifiée (GUI)
- Connectivité aux sources de données les plus courantes (LDAP, SQL, Active Directory…)
- SDK/REST API

**MANAGEMENT**
- Portail captif
- Services DNS, DHCP, RADIUS embarqués
- Traçabilité complète et exhaustive
- Mise en place sans agent

**EXPLOITATION**
- Administration à distance
- Découverte et inventaire temps réel
- Déploiement en deux phases sans impact
- Support de la virtualisation
- Information dynamique de l’administrateur

**ROBUSTESSE**
- Système d’exploitation éprouvé
- Module de Haute Disponibilité
- Délégation d’administration fine
- Gestion d’accès et contrôle d’utilisation
- Option de by-pass pour les Appliances

**FLEXIBILITÉ**
- Architecture modulaire évolutive
- Moteur de génération de rapport spécifique
- Paramétrage des politiques de sécurité
- Disponible en image logicielle ou préchargée sur un serveur (appliance)

**PERFORMANCE**
- Fonctionnement garanti avec tous les fournisseurs respectant les normes*
- Testé avec plus de 1000 équipements connectés simultanément
- Supporte un débit de plus de 3000 requêtes à la seconde (v1.3)
- Capacité de gestion multisite (v.2)
Thank you!