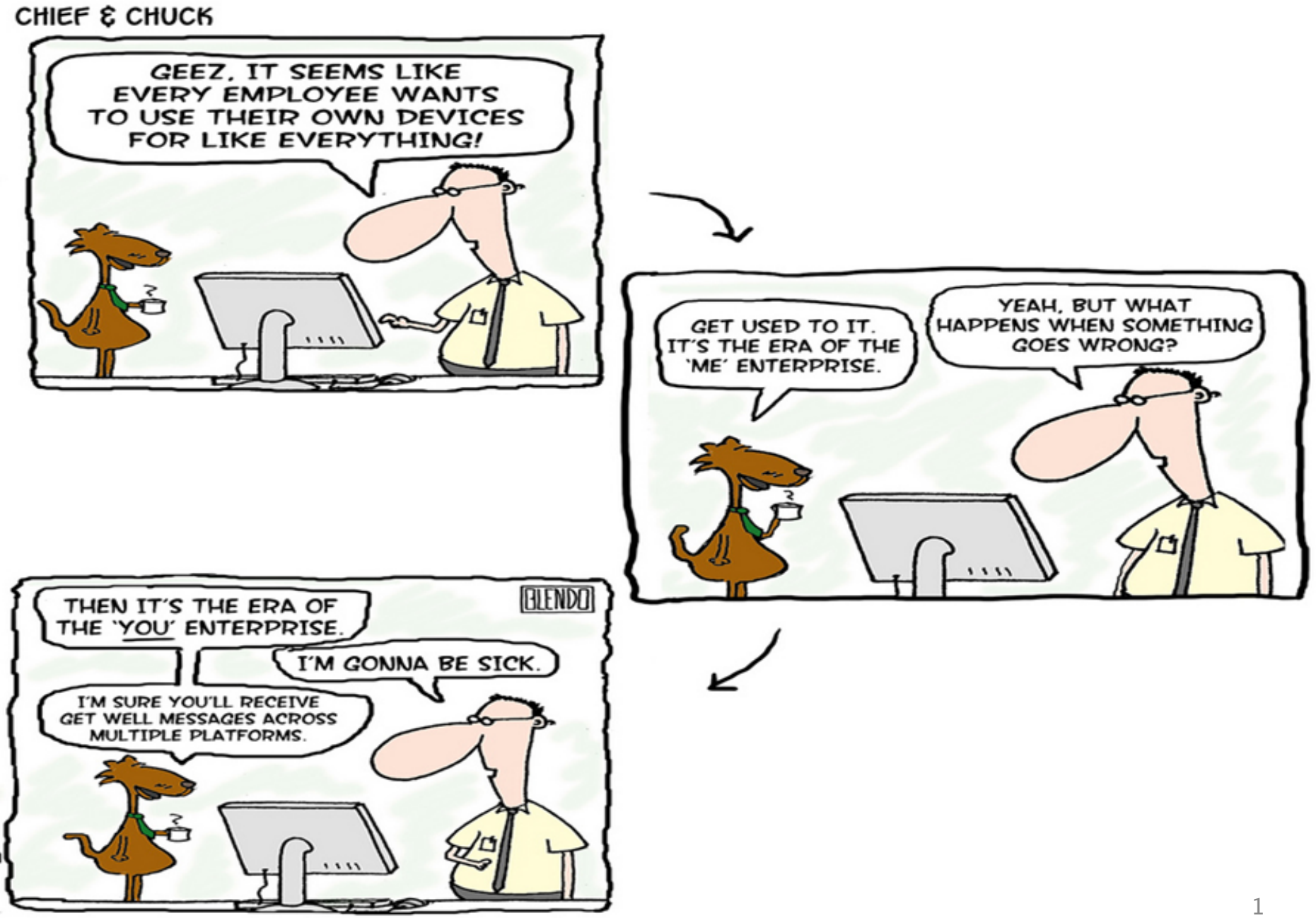

CHIEF & CHUCK
GEEZ, IT SEEMS LIKE EVERY EMPLOYEE WANTS TO USE THEIR OWN DEVICES FOR LIKE EVERYTHING!
GET USED TO IT. IT'S THE ERA OF THE 'ME' ENTERPRISE.
YEAH, BUT WHAT HAPPENS WHEN SOMETHING GOES WRONG?
THEN IT'S THE ERA OF THE 'YOU' ENTERPRISE.
I'M GONNA BE SICK.
I'M SURE YOU'LL RECEIVE GET WELL MESSAGES ACROSS MULTIPLE PLATFORMS.
BLENDO

How BYOD has changed the security map of enterprises and how “Peregrine Guard” help tackle it?

By Manjunath M Gowda, ceo i7 Networks

Summary of the Deck

- Security Problem due to BYODs
- How do we Solve?
- How are we different?
- What we find
- Deployment
- How we differ with competition?
- Current product status
- How we use Azure and Adv. Of Azure

Problems due to BYOD

BYODs bring in three issues mainly…

- Attacks on corporate network (& data loss) can come via
  - **Unauthorized & insecure devices,**
  - **Compromised/malicious devices,**
  - **Older & vulnerable OS & apps**
  - **Non-integrity devices (jailbroken/rooted), and**
- Unable to control access to internal data from these devices. Role-based privileges are **not enough**.
- Stolen/Lost devices with corporate data on it.

How we solve?

- **A**uto-detection of all devices
  - Irrespective of how they join or try to join the network (Regular, Unauthorized (Spoofing/Hot-spotting etc.))
- Auto-check on health of the device such as
  - compromised devices (including jailbroken/Rooted)
  - those below corporate suggested baseline
  - those with vulnerable OS/Apps
  - those that are malicious (malicious traffic)

How we solve?

- Give a vulnerability index to each of the device (DVI^{tm})
- Policy Enforcement (Allow/Deny/Differential Access) using DUAL-TIER

How we solve? (Optional)

- Strong Authentication via AD or RADIUS or LDAP
- Differential access to assets based on user, role, device, location, branch-office, Apps and other parameters (DUAL-TIER).
- Ensuring that no access to corporate network until it is registered with EAS (or any MDM solutions) and hence providing that "Safety Net"
- Integration with EAS or other MDM solutions ensures remote wipeout.
- Also integrating with MS InTune

How do we do? How are we Different?

We do all of it :

- Completely Agentless and non-intrusive
- Don't even ask devices to go to a self-registration portal
- Provides a "safety-net" to enterprises by pulling all devices to management.
- Being client-less also helps EU Data protection act to a great extent

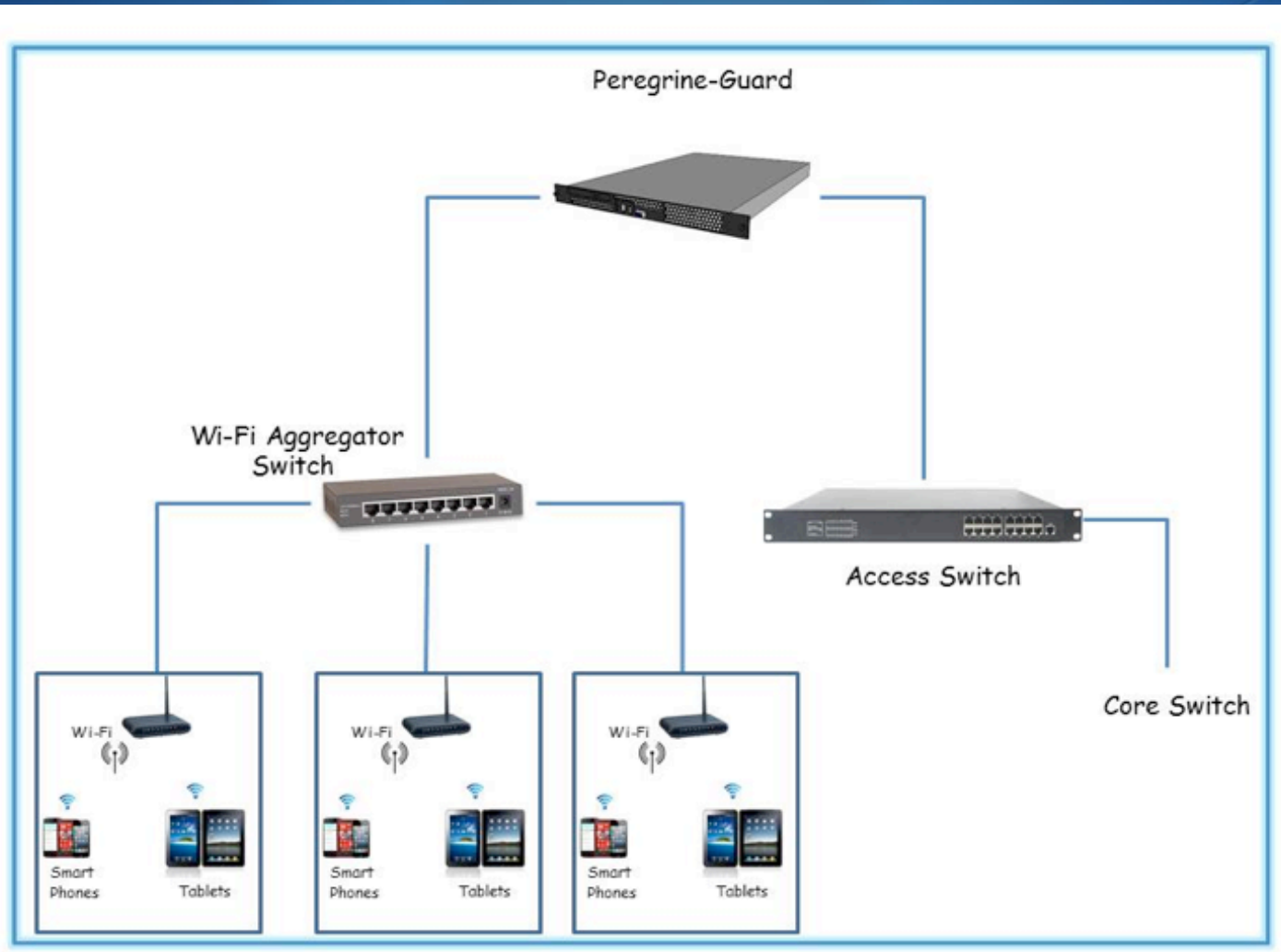
What we find?

- Deterministic (before/when they connect)
  - Mac-id, OS (iOS or Android etc.), Device kind (iPad v/s iPhone etc.)
- Heuristic (while they operate)
  - Jailbroken/rooted
  - Malicious traffic
  - OS version
  - Malicious Apps, &
  - Vulnerability Index

Deployment

- Probes all over the network behind all main network aggregate points (wired and Wi-Fi) in passive mode (for Discovery)
- Policy enforcement appliance in-line and behind main Wi-Fi aggregator.
- **DIRISC**: easily **D**eployable, **I**nvisible, less **R**esource intensive, **I**ntegrates well with the existing infrastructure, easily **S**calable, & truly **C**ross-platform.

Deployment



How are we differ with competition?

WE	Competition
⊙ Agentless and Non-Intrusive. ⊙ Auto device enrolment/on-boarding	⊙ Agent (client) based ⊙ Require on-boarding of devices ⊙ Visiting a self-registration portal
Covers to all devices (Heterogeneous)	Only managed devices
Detect backdoors, spoofs (MAC-id, IP, Hotspots).	Not done/not applicable
Supports ANY connected devices	Only support of smart mobile devices/ OS for which they have clients
⊙ Reports Network behavior patterns ⊙ Recognizes malicious traffic & anomalies	No tracking of network usage patters or anomalies.

How are we differ with competition?

WE	Competition
Check device health including detecting jailbroken, rooted & compromised devices	With agents and again only for managed devices.
Cross-platform, scalable and less resource intensive. Easy to provision.	⊙ Device/OS specific solutions. Provisioning can be cumbersome. ⊙ Not scalable & highly resource intensive.
Absolutely no change in user behavior or user experience;	Changes in the profile, user behavior, user experience

Current Product Status

- Available in two flavors:
  - Just the discovery module (PG lite) – deployed passively.
  - Both discovery and policy enforcement modules – deployed inline mode
  - Supported platforms: Windows, Linux and FreeBSD
- Beta version: April 7, 2013
- GA : by Mid of May, 2013
- We are demoing and announcing the launch in CITE conference June 1-3, 2013 @ SFO

How do we use Azure?

- PG was built over FreeBSD but has been ported to Linux and Windows
- i7 Networks got selected as final 13 among 500 companies by the **MS Azure Accelerator Program** and we are deploying the same on Azure
- We needed a Strong Authentication and Active Directory provided the right way and Azure AD was far easier for us to integrate (Work in Progress)

How do we use Azure?

- We are also integrating all our reporting into Azure to provide one single centralized reporting on the cloud (Work in Progress)
- It supports Linux VMs too and hence made our life easy to setup testing on multiple test beds
- Azure Accelerator program needs first rights and hence cannot show the integrations or snapshots yet ☹

Azure learning's…

- Easy to deploy and run Windows Server and Linux virtual machines.
- Migrate applications and infrastructure without changing existing code
- Process, analyze, and gain new insights from big data using the power of Apache Hadoop. (to store mobile data and draw analytics)
- **Mobile Services** – to build app so that we can do a reporting app with role based access for reports

Working with MS..

- Early stages on working integrating our solution into Systems Center
- Early stages again in working with integrating our solution into MS InTune, their MDM solutions
- Integrated with Azure AD
- Working with integrating into MS EAS so that we provide safety net for getting all devices under EAS

Questions?

URL: www.i7nw.com
email: info@i7nw.com, info@i7nw.eu
Blogs: i7nw.com/blogs
Video: http://youtu.be/aHGyAfIWUps
my email id: manju.m@i7nw.com