



## **Security: *Locked Down but Not Locked Out***

Live Webinar | February 17<sup>th</sup> 2010

Ron Golesh | Maron Structure Technologies

# Meeting Agenda

- Overview of security concerns for voice and mobility solutions
- Network concerns
- Physical concerns
- Policy Management for Unified Communications
- Scenarios and Use Cases
- Mobile security roadmap



# Key Mobile Security Concerns

- **Exposure of critical information:** Small amounts of WLAN signals can travel significant distance, and it's possible to peep into these signals using a wireless sniffer. A wireless intruder could expose critical information if sufficient security isn't implemented.
- **Lost or stolen devices:** Even if sufficient security is implemented in wireless virtual private networks (VPNs), if a device is lost or stolen, the entire corporate intranet could be threatened if those devices aren't protected by password and other user-level security measures

# Key Mobile Security Concerns

**Mobile viruses:** Mobile viruses can be a major threat, particularly with devices that have significant computational capabilities.

Mobile devices, in general, are susceptible to viruses in several ways:

- Viruses can take advantage of security holes in applications or in the underlying operating system and cause damage
- Applications or applets downloaded to a mobile device can be as virus-prone as desktop applications
- In some mobile OSs, malformed SMS messages can crash the device.

The 911 virus caused 13 million i-mode users to automatically place a call to Japan's emergency phone number.

# Key Mobile Security Concerns

**E-mail viruses:** E-mail viruses affect PDAs in much the same way regular e-mail viruses affect PCs (i.e., causing the PDA e-mail program to send multiple e-mails). These viruses are costly to enterprises and interrupt normal business too. PalmOS/LibertyCrack is an example of a PDA e-mail virus. It's a known Trojan horse that can delete all applications on a Palm PDA.

**Spam:** Spam causes disruption and drives up costs when it's targeted toward wireless devices

**Source: Nemertes Communication and Computing Benchmark 2009**

# Actions You Can Take

Use **advanced encryption and key management techniques** to minimize WLAN-related security vulnerabilities. High-level security is available for WLANs using features such as Internet Protocol Security (IPSec) and 802.11 security standards such as EAP and WPA, WPA2, NAC (Not WEP).

**Put strict access privileges on mobile users** to protect sensitive information.



# Actions You Can Take

## **Create security policies specific to mobile device usage.**

Minimize the impact of a lost device: **Password-protect all devices**, encrypt sensitive documents on the device, and don't use automatic scripts for VPN login. Mobile device security policies should also include minimizing access to limited sources using firewalls.

**Regularly back up** PDA/Smartphone/Laptop data to a PC to prevent damage from PDA-specific viruses and worms.



# Actions You Can Take

Use antivirus software for PDA/Smartphones. **Network-level scans are the most effective**, centralized way of preventing viruses and other disruptions associated with mobile devices.

Access control should include both hardware/device-based authorization and application based authorization.



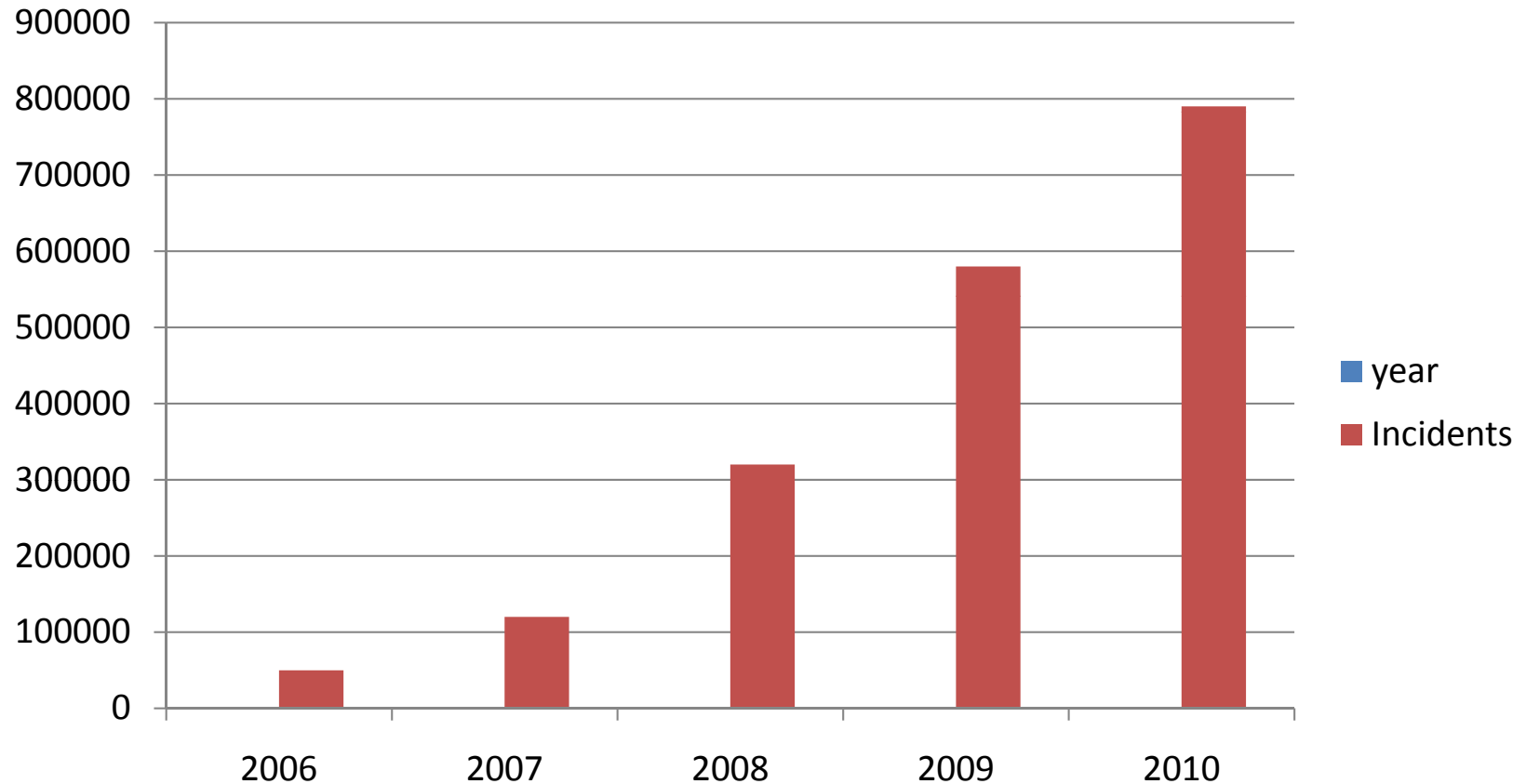
# Actions You Can Take

**Provide specialized training to mobile device users** and administrators, including simple guidelines for the physical security of devices and a reporting mechanism in case of loss or theft.

**For virus/spam protection**, customer premises solutions (or behind firewall solutions, as they are called) are more effective than similar solutions hosted by the mobile carrier. Firewall solutions are much easier and effective to control and manage.

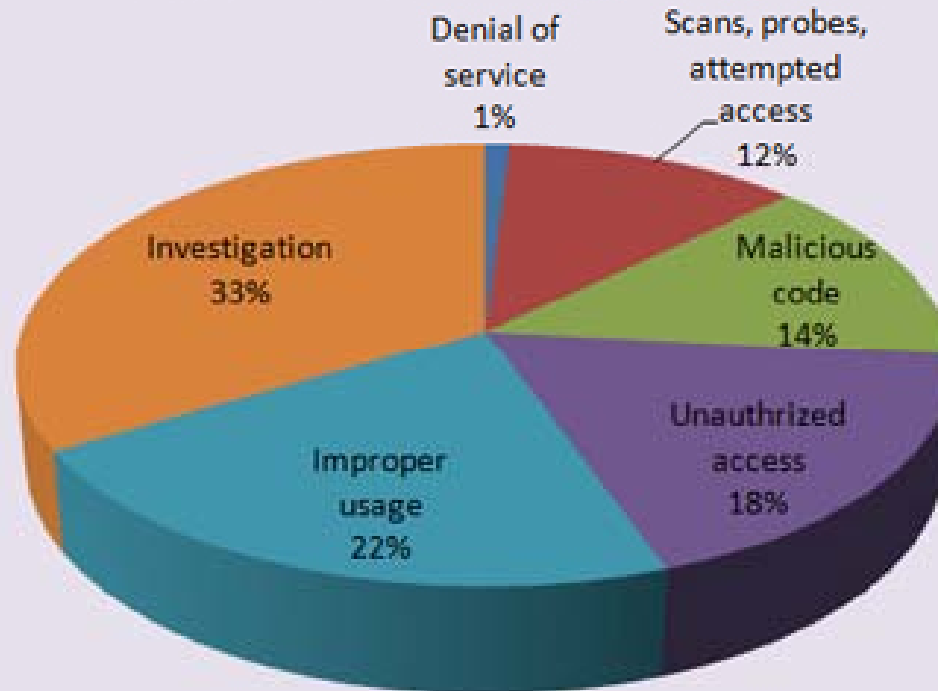
# Increases in Incidents 2006 to 2010

## Cyber Incidents reported to US-CERT

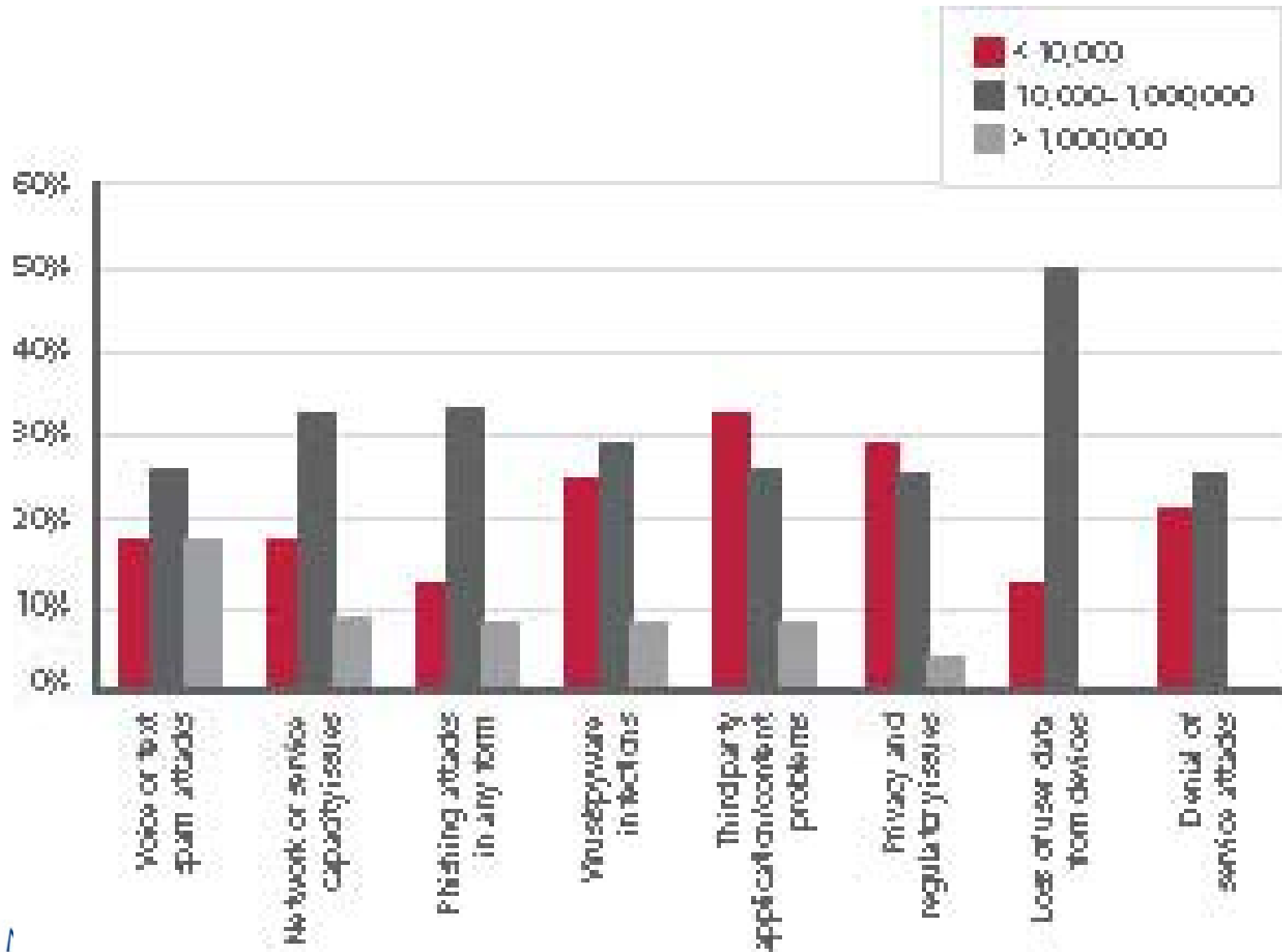


# Incidents Reported

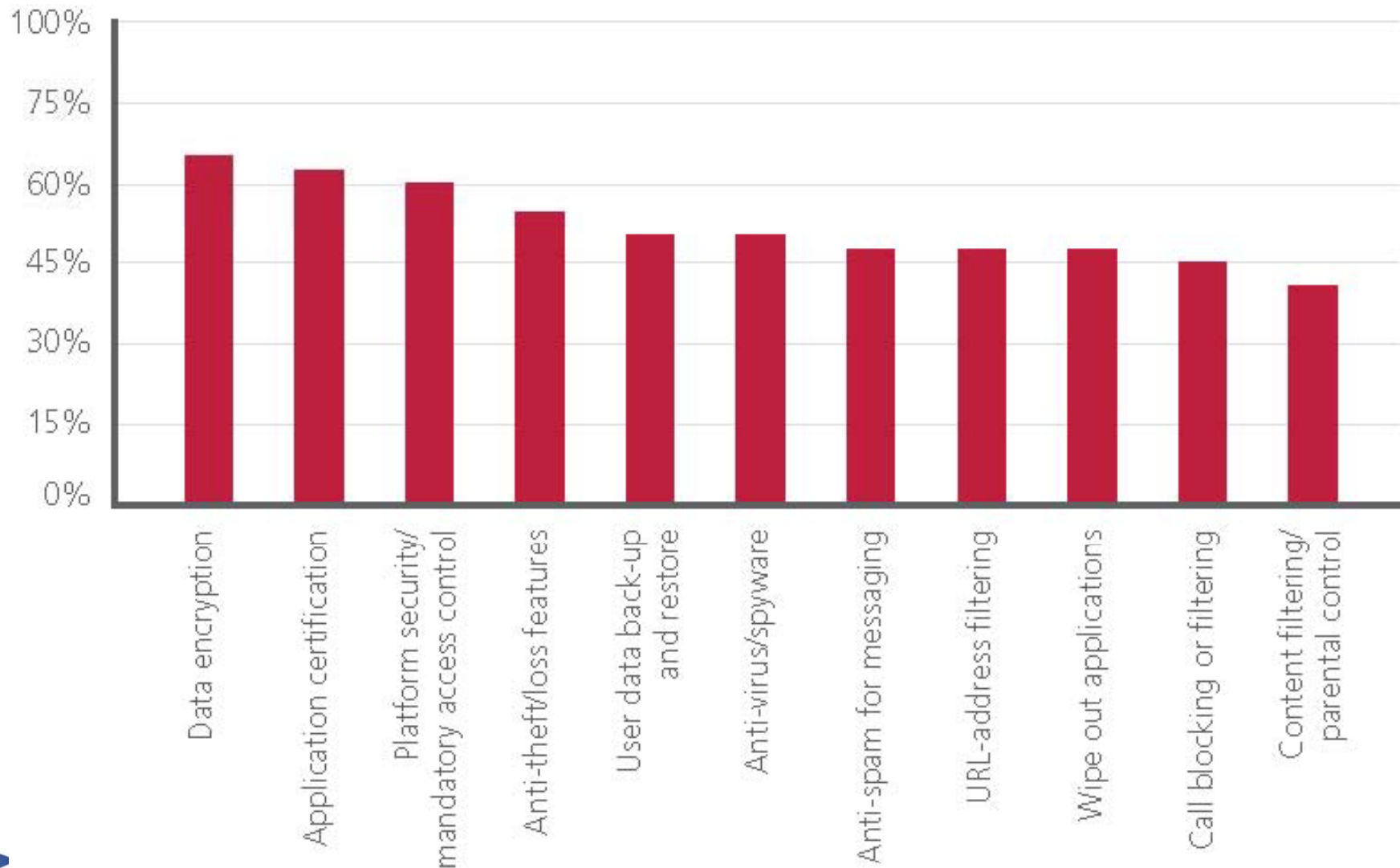
**Percentage of Incidents Reported to US-CERT in FY06-FY08 by Category**



# Number of Devices by Incident Type



# Security Features Implemented



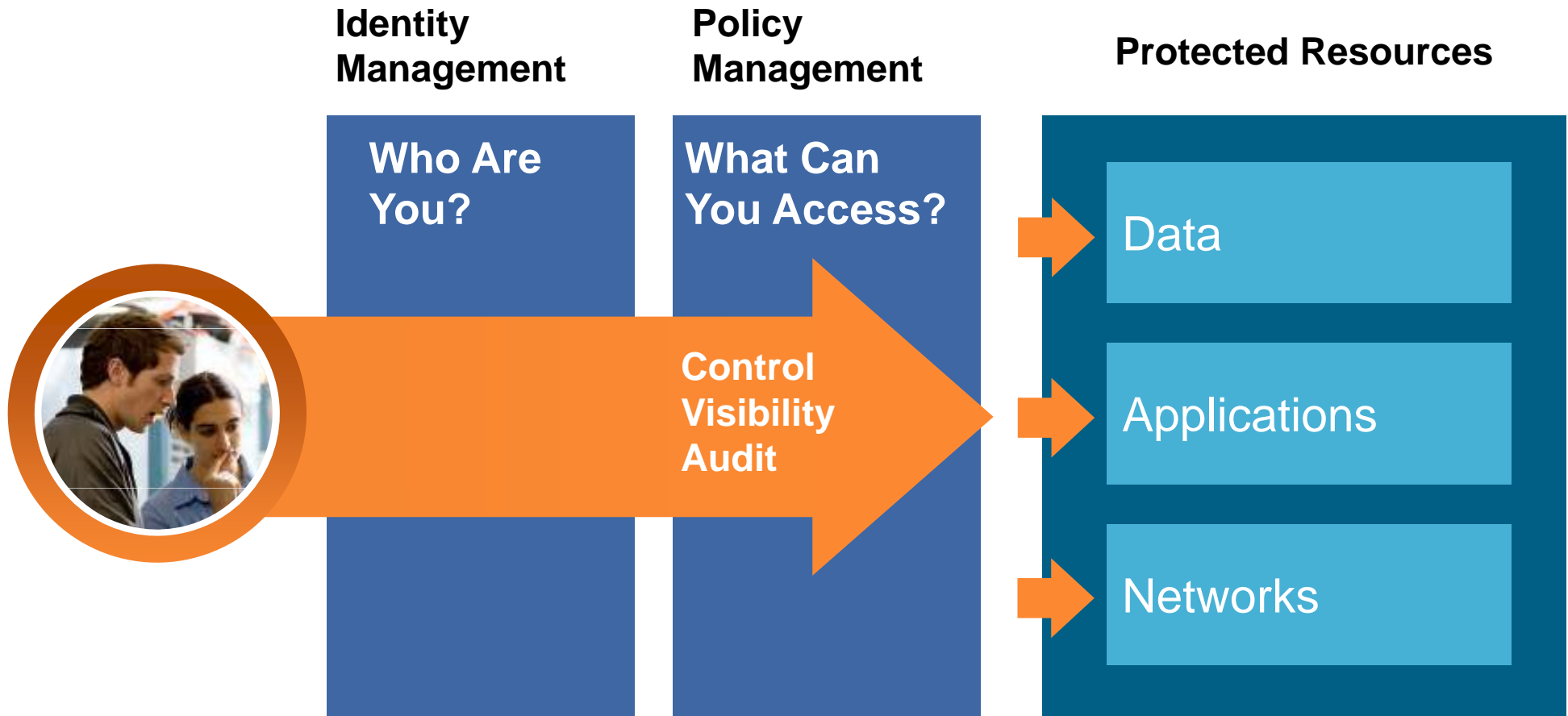
# Who Does Security Affect?

- **Financial Services: Can a trader place a trade?**
  - Given the dollar amount of the trade
  - Given the time of day
  - Given the instrument being traded
- **Healthcare: Can your spouse access your personal health records?**
  - Given the nature of the information
  - Given your permissions
- **Technology: Can a user access a product design document?**
  - Given their role if they are an outsourced employee
  - Given the authentication method used
- **Government: Can an intelligence officer access threat database?**
  - Given their affiliation and pre-existing arrangements
  - Given their clearance level
  - Given which network they are accessing it from

# Value Proposition

- Consistent administration and enforcement of entitlement policies (“configure not code”)
  - Centralized, delegated management useable by non-developers
  - Consistently applied for local, and remotely hosted, resources
- Centralized auditing and real-time remediation
  - Policy what-ifs
  - Comprehensive who has access to what, and, who did access what
- Enterprise-class, standards-compliant product with out-of-the-box integration with existing customer infrastructure
  - Scalable from single application, to heterogeneous LoB, to globally distributed enterprise

# Policy Management



# Unified Communications Architecture

End User Clients



## Collaborative Applications

UC or UM apps

Partner Apps

Customer Apps

## API

Call Control

Voice

File Mgmt

Video

Directory & Identity

Data Sharing

Presence & Location

Routing & Queuing

IM & Chat

Custom Data

Policy Mgmt

Global Delivery Network

# Policy for Unified Communications

- **Control entry, initiation or access to something**

Examples: Meetings, messages, documents, and communication with individuals

- **Information sources**

Job role, organization, and other directory attributes

Presence

Application specific attributes

*Physical geographic location*

*Mode of access to network*

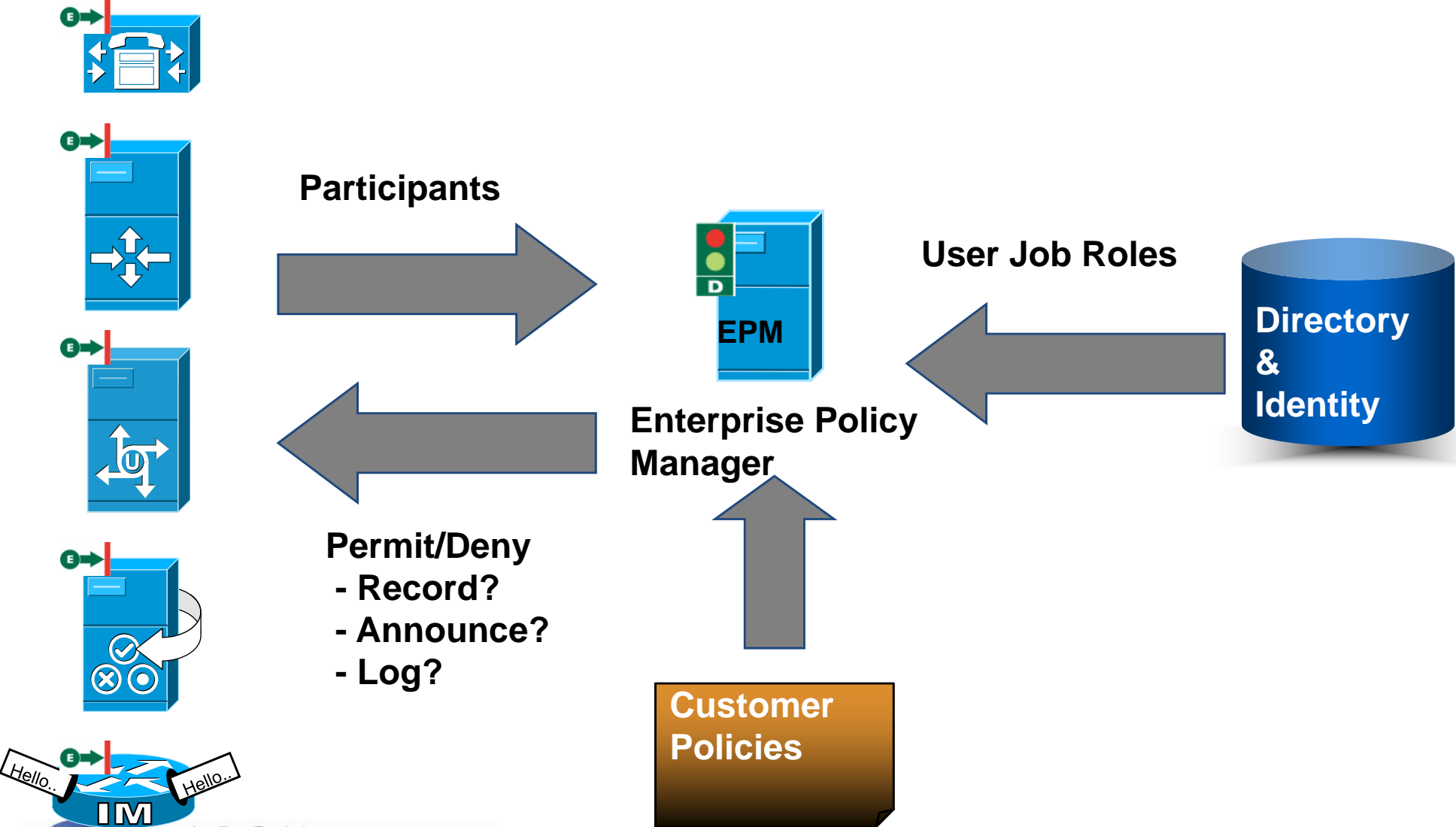
*Time of Day & Day of Week*

*Calendar entries*

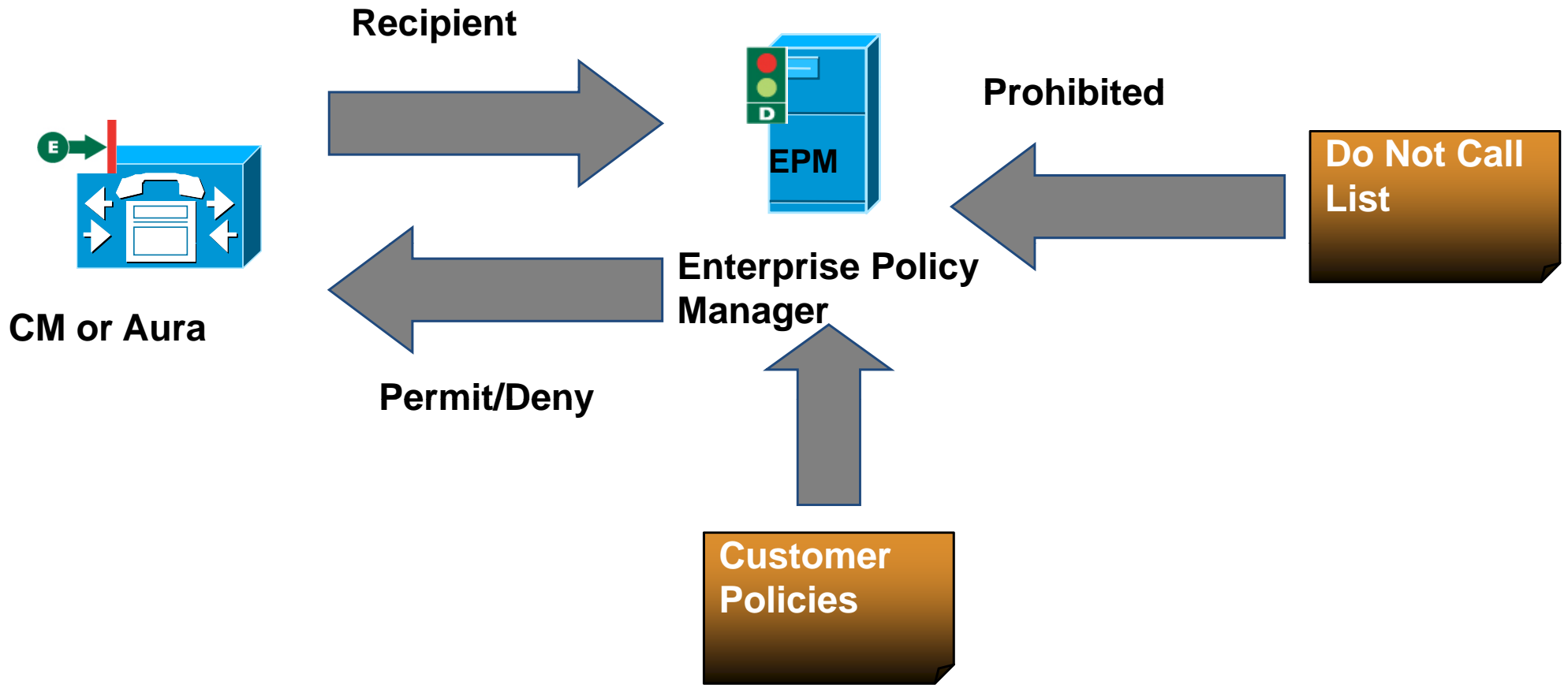
- **Controlling additional behaviors as obligations**

Examples: Record, audit, send email, and require acknowledgement

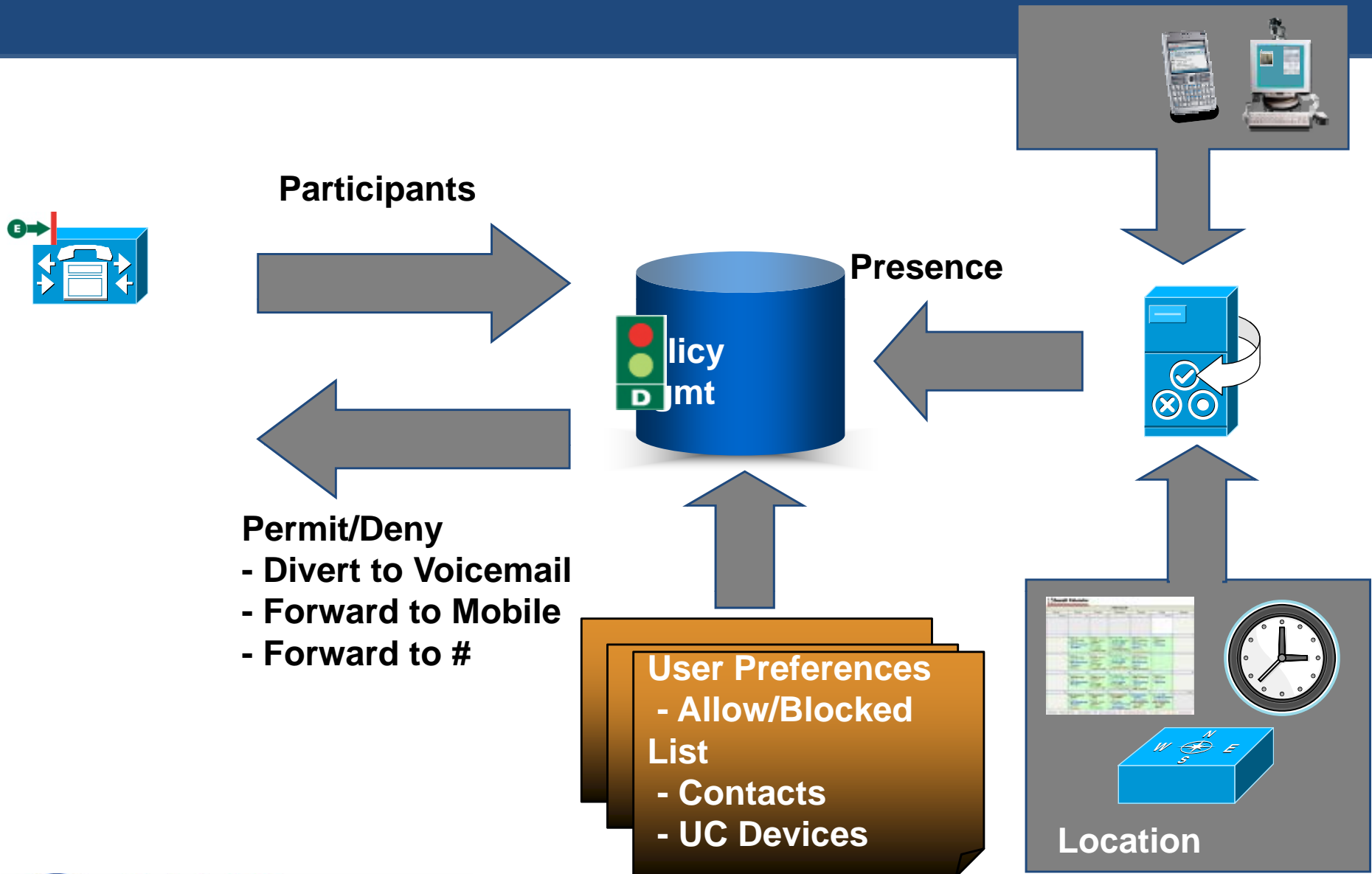
# Corporate Policy - Ethical Wall



# Corporate Policy - Do Not Call List

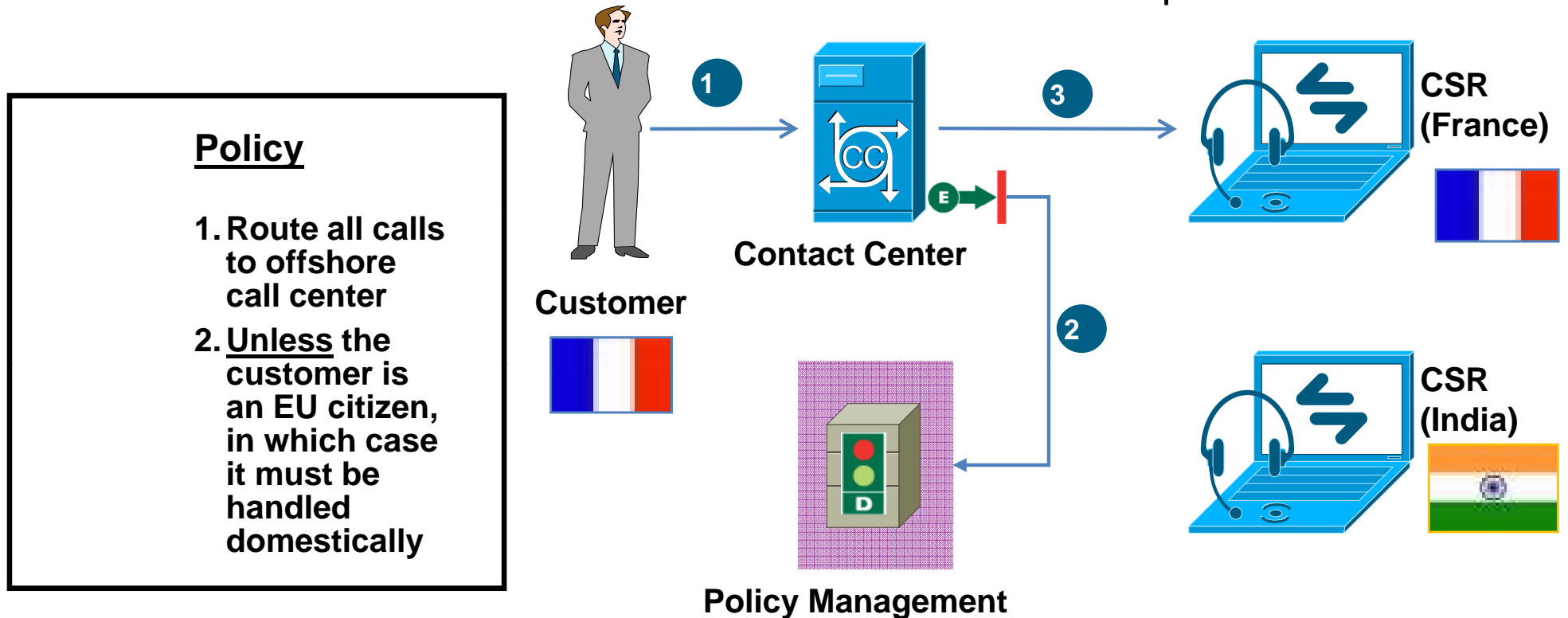


# User Preferences - Presence Enabled Routing



# Policy-Based Call Routing

1. Call center receives customer call from a French national
2. policy check
3. Call routed onshore vs. offshore based on customer preference



# Secure Voice: Today.....



# Secure UC

- Security is about enforcing policies where/when needed
- Enforcing security policy is *Imperative*
- Defense-In-Depth is *Imperative*
- It's not *just* about protecting the Aura or for that matter Microsoft OCS

# Questions To Ask Yourself

- What's your UC security strategy?  
What groups are involved in that strategy?
- How are you meeting regulatory/legal requirements as you roll out UC?
- How will you enforce policy – ie. who talks to whom and when?
- Is encrypted voice important?  
If so, how will you inspect the traffic?
- How will you secure your mobile UC?
- How will you handle UC & Security in branch offices?
- What is your defense-in-depth approach to UC?

# More Steps to Take

## **Applications**

- Robust secure messaging

- Ability to use firewall security policies on UC applications

## **Endpoints**

- Inspection of phones

- Mobile secure UC

- NAC for phones

## **Call Management**

- Inspection of encrypted voice and video traffic

- Integrated Behavior-based control on servers

## **Infrastructure**

- Separation of voice & data traffic (VLANs)

- Bandwidth management for all types of applications

- Integrated Voice and Security (VSEC Router bundle) for branch offices

# Microsoft OCS Security Guide

## Oct. 2008 Highlights of Analysis

	<b>Microsoft</b>
	<i>Insists on encryption for all traffic. At odds with customers needing to inspect local UC traffic.</i>
	<i>No ability to inspect encrypted UC traffic.</i>
	<i>Network DoS not addressed.</i>
	<i>Managing settings &amp; services.</i>
	<i>No protection against 'day zero' attacks.</i>
	<i>MS mentions need to 'address threats to core infrastructure,' but offers no core infrastructure security.</i>
	<i>Recommends disabling services not required for OCS. Doesn't say which ones.</i>

# MONSANTO

## Opportunity: Voicemail

- Replace aging Octel voicemail system
- Business Decision Makers wanted Unified Messaging
- Microsoft pitched “free” Exchange 2007 UM
- Monsanto Legal required different discoverability policy for voicemail vs email when sharing the same message store
- Module Messaging met this requirement and also provided message encryption

# MONSANTO

## Opportunity: Conferencing and Web Collaboration

- Replace aging conference bridge
- Due to an impending two-year interstate project, the Business wanted to provide remote collaboration solutions for at-home workers
- Microsoft pitched “free” Live Meeting – customer still needed an audio conference bridge
- Live Meeting DMZ servers rely on AD authentication. There is direct access to internal AD accounts in the DMZ. Denial-Of-Service attack could lock user’s internal AD account if too many invalid logins are attempted. Brute force password attacks were possible.
- Avaya keeps internal meetings and user passwords off of the external web server.

# Proven Enterprise Deployments



Welcome to Smart Technology.  
[www.structure-tech.com](http://www.structure-tech.com)

# Conclusion

**Question and Answer Session**

**Thank you for your time.**



**Welcome to Smart Technology.**  
[www.structure-tech.com](http://www.structure-tech.com)