Rethinking Enterprise Security

Toby Kohlenberg
Senior Information Security Technologist
Intel Information Risk and Security

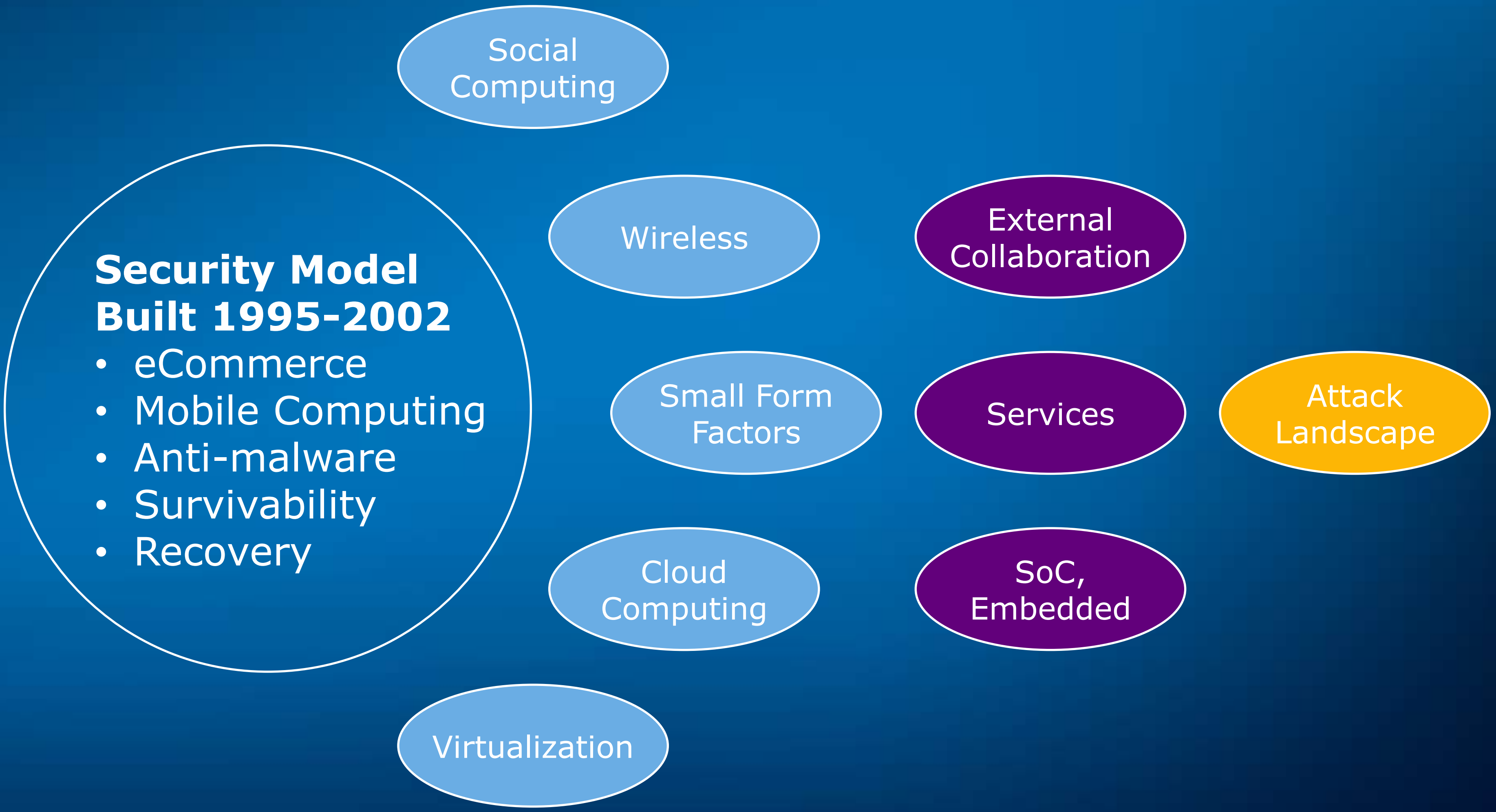
January 28 2012

IT@Intel

Agenda

- Problem Statement – New Problems, Old Solutions
- Approach – Blank slate
- Process – Targeted group/methodology
- Solution
- Progress to date
  - Successes
  - Challenges
- Key Messages

Problem – The Old Security Model Didn't Scale



Security Model Built 1995-2002

- eCommerce
- Mobile Computing
- Anti-malware
- Survivability
- Recovery

Social Computing

Wireless

External Collaboration

Small Form Factors

Services

Attack Landscape

Cloud Computing

SoC, Embedded

Virtualization

IT@Intel

Idea - Approach & Team

- If we were starting from scratch what would we do differently?
- Small, focused team
  - Multiple disciplines
  - Must have tactical knowledge, capacity for strategic vision and be open to confrontation
  - Whole team must agree before adding additional team members
  - Management had no say as to who was on the team
- Expectation that we might not come up with anything

Process

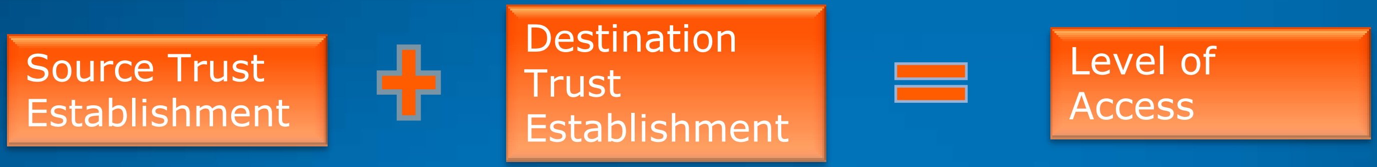
- 7 of us locked in a room for a week
- Leave egos outside the room
- Slide a pizza under the door periodically
- What happens in the room stays in the room
- Brainstorm, argue, complain about what we have today

This was just the beginning of the journey.

The solution

- A new approach and architecture based on four ideas
  - Dynamic Trust Calculation
  - Isolated Security Zones
  - Aggressively balanced controls
  - Additional “perimeters” added
    - User
    - Data
- Ongoing coordination and guidance by the original core team to keep the momentum and the right direction
  - Spin off separate teams to research/implement specific features/capabilities

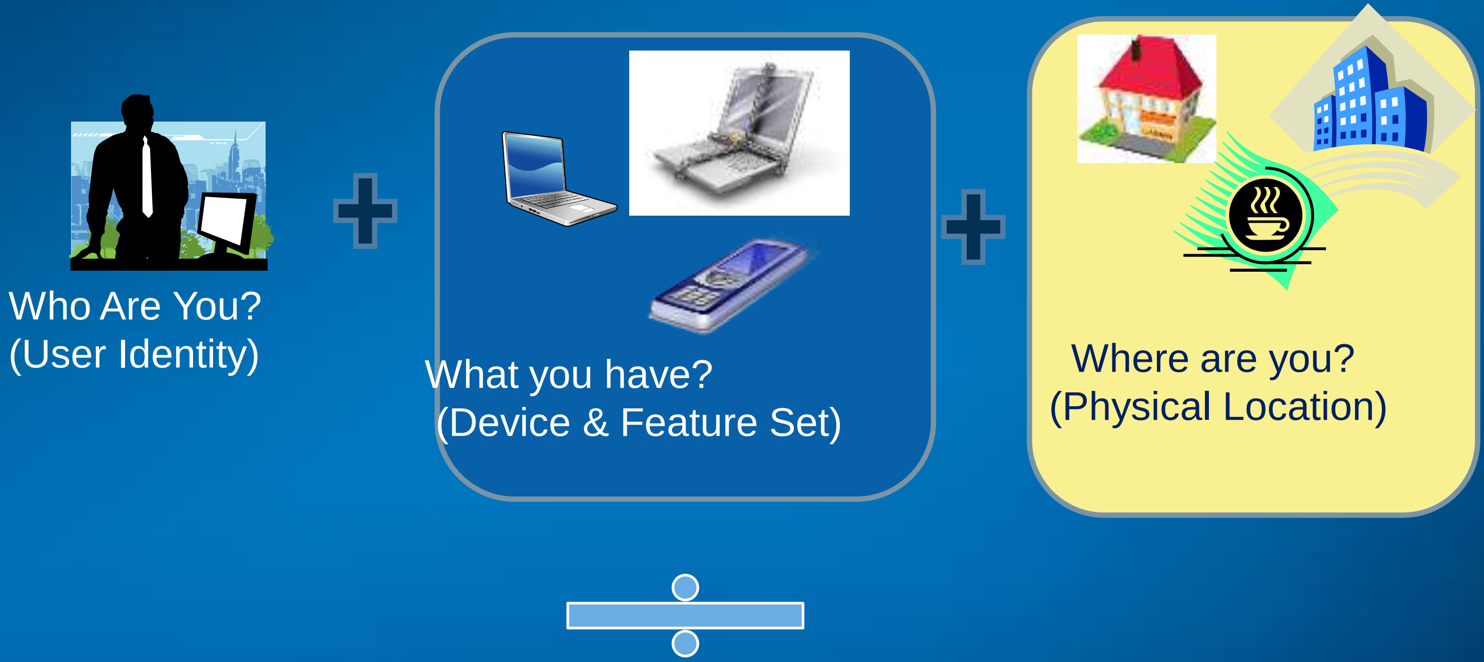
Dynamic Trust Calculation



Source Trust Establishment + Destination Trust Establishment = Level of Access

- Recalculated as necessary
  - Session (re)establishment
  - Detective control feedback loop
  - Change in any trust calculation characteristics

Source Trust



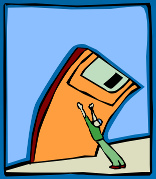
Who Are You?
(User Identity)

What you have?
(Device & Feature Set)

Where are you?
(Physical Location)

Data confidence

Destination Trust



Who You Are?
(Receiving application)

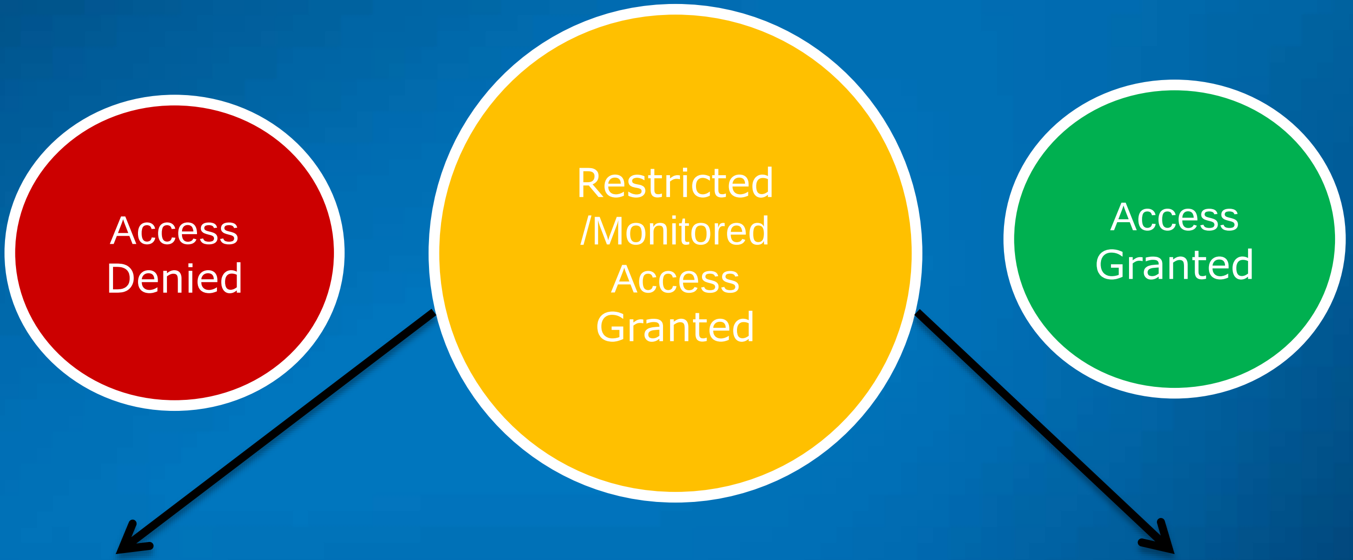
+

What do you want?
(Data Classification)

+

Where is the data?
(Data Location)

Resulting Access



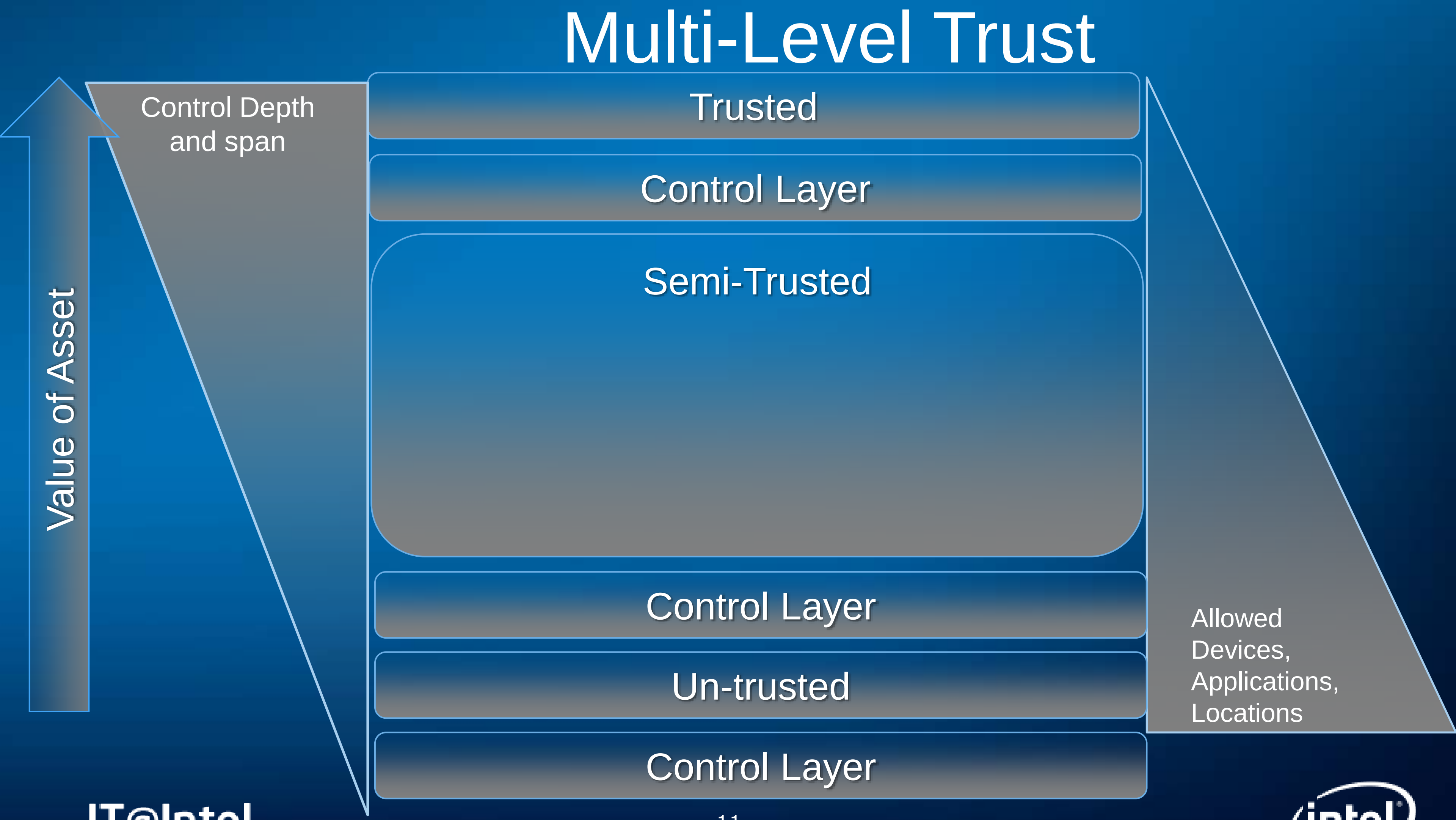
Access Denied

Restricted /Monitored Access Granted

Access Granted

- Change in access method
- Reduction in access
- Increase in logging

Isolated Zones



Multi-Level Trust

Value of Asset

Control Depth and span

Trusted

Control Layer

Semi-Trusted

Control Layer

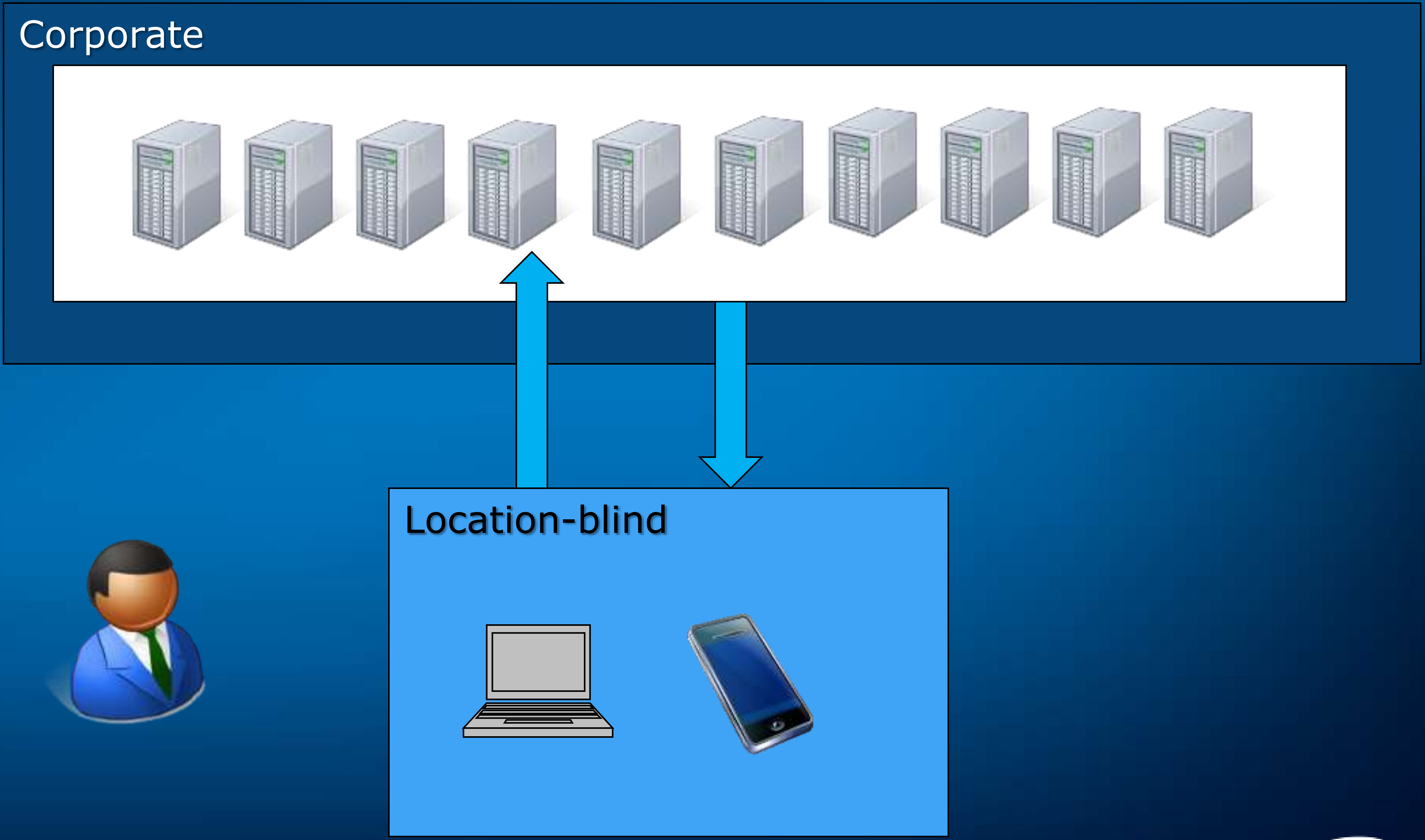
Un-trusted

Control Layer

Allowed Devices, Applications, Locations

IT@Intel

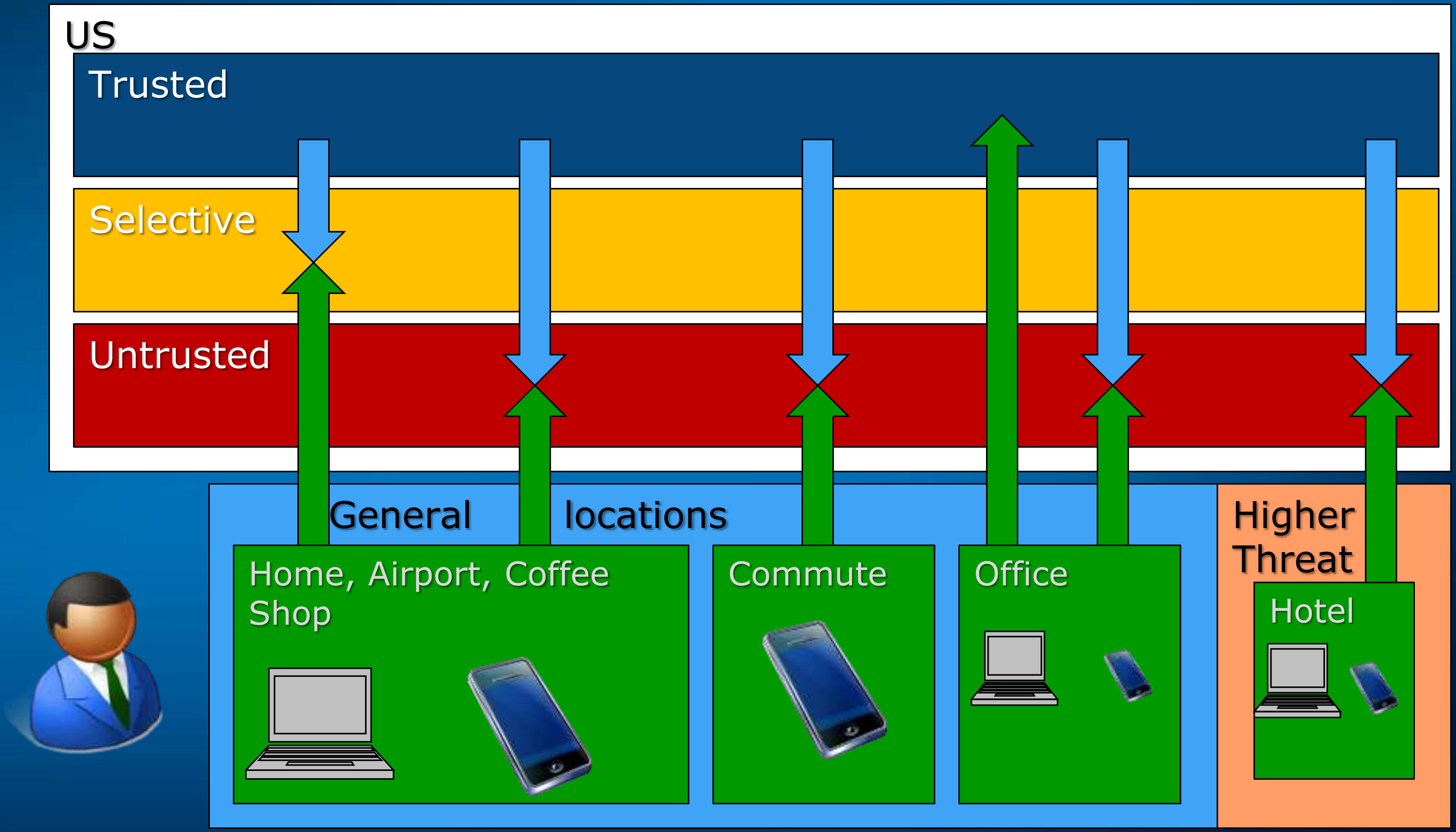
Current Model



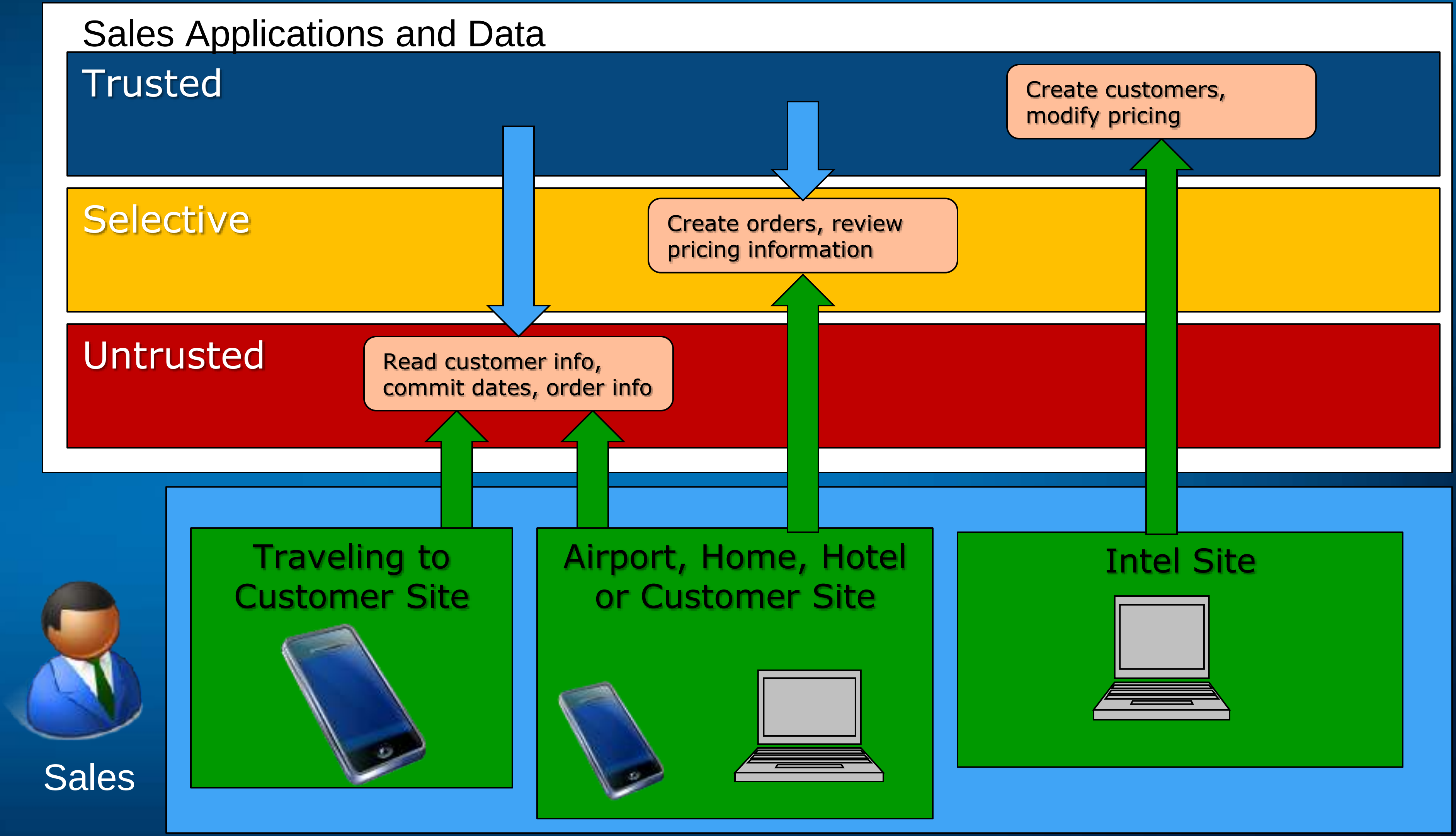
Corporate

Location-blind

General User Example (Day in the Life)



Sales Force Example (Day in the Life)


Sales Applications and Data
Trusted
Create customers, modify pricing
Selective
Create orders, review pricing information
Untrusted
Read customer info, commit dates, order info
Traveling to Customer Site
Airport, Home, Hotel or Customer Site
Intel Site
Sales

Balanced Controls

- Enterprises have been focusing on prevention for a long time
  - Appealing – it really does save money if it works
  - Common sense
  - **Only works when you aren’t allowing things.**
- Instead look at aggressive monitoring/detection and correction
  - Allow for false positives by using granular, scaling responses
    - Increased logging
    - Activity throttling
    - Increasingly granular role-back/journalling
  - Plan for compromise
    - Hence detection and recovery

Successes to date

- Creation of a dedicated (separate) program for implementing the infrastructure changes required
- Driving the idea of trust zones across IT
  - Partnering with our remote access engineering and small form factor engineering teams has given high ROI.
  - The Virtualization High Trust Zone is the first implementation of complete trust segmentation
- Proof of concept of dynamic access calculation
  - This is being deployed in 2012.
  - Building in-house, evaluating options for production solution.

(more) Successes to date

- Creation of User Security dashboard
  - Show the user where/when they are logged in, let them help us find suspicious stuff
    - Also helps with debugging and explaining when their access fails
- Driving the idea of balanced controls across IT
  - Leveraged InfoSec org to push this
  - Working closely with engineering teams to ensure smooth implementation
- Very positive vendor response to the idea
  - Many are already working on pieces of the idea
  - Some are starting to publish their own versions of our work

Challenges (and solutions) so far

- The team that created this are already busy with their full-time jobs
  - Once the idea had support, a full separate program was created to push the idea "Security Transformation". This let the core team keep focusing on driving the idea. Other project teams are spun off as necessary.
- Vendors are just starting to talk about some of the features we need
  - So we are building pieces ourselves and we're working to influence the ecosystem (and asking others to also)
- Users get confused when access works some of the time
  - Focus on transparency and user communication as well as extensive logging

Challenges (and solutions) so far

- Apps can’t implement the trust model before clients can provide the data before apps implement the …
  - We are bridging some of it with proxies that can implement the features and setting corporate direction to force the changes we need
- Some of these things are obvious – so why aren’t they common?
  - Need a single group with the political (and real) capital to make them happen, and the long term focus to stick with it.
- The dynamic trust adds massive complexity
  - So we are starting with simple versions to keep this debugable over the long term

Challenges (and solutions) so far

- Requires massive coordination/influence
  - Getting new enabling systems built
  - Getting new projects to go in the right direction
  - Getting existing projects to migrate to the new model
  - So we kept the core team small and tightly coordinated and fully bought in on all decisions.
    - This allows each member to work on separate issues independently.
  - Extended teams are used to do specific work
- Many of the problems aren't technical – legal, usability, etc…
  - Take the time to think about them and pull in experts to help
- Some capabilities will take years to implement so we have to start long before we "need" them
  - Which is a key reason this is an ongoing program – to maintain the vision and funding

Benefit to Intel

- Flexible and Extensible
- Consistent
- Improved Granular Controls and Access Methods
- More aggressive IP protection
- User Flexibility
- Increased Productivity
- Enables new customer driven usage models and Faster Adoption without having to accept additional risk

Want to know more

- http://www.intel.com/itcenter/itatintel/index.htm
- *"Rethinking Information Security to Improve Business Agility"*
  - http://download.intel.com/it/pdf/Rethinking_Information_Security_Improve_Business_Agility.pdf
- Search for "rethinking" "security" "intel.com"
- If this is interesting and you have thoughts, let me know
  - toby@intel.com

intel®