Publishing Enterprise Web Applications to BYOD using a Granular Trust Model

Shachaf Levi
IT Client Security & Connectivity
May 2013

IT@Intel

Legal Notices

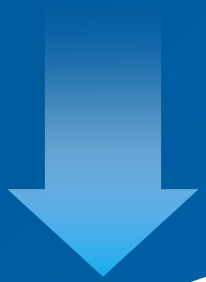
This presentation is for informational purposes only. INTEL MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Agenda

- IT Risk And Security ‘A Balancing Act’:
  Protect to Enable
- Solution:
  - Access Web applications based on dynamic and granular security controls
  - web applications‘ mobile friendly UI
  - Seamless OTP Authentication
    and Single-Sign-On using Kerberos

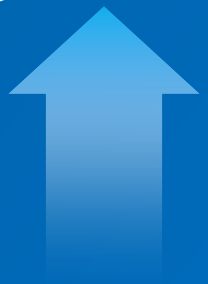
IT Risk And Security 'A Balancing Act'

Open Access
Controls increased cost and constrains use of data and systems



How Do We Balance?

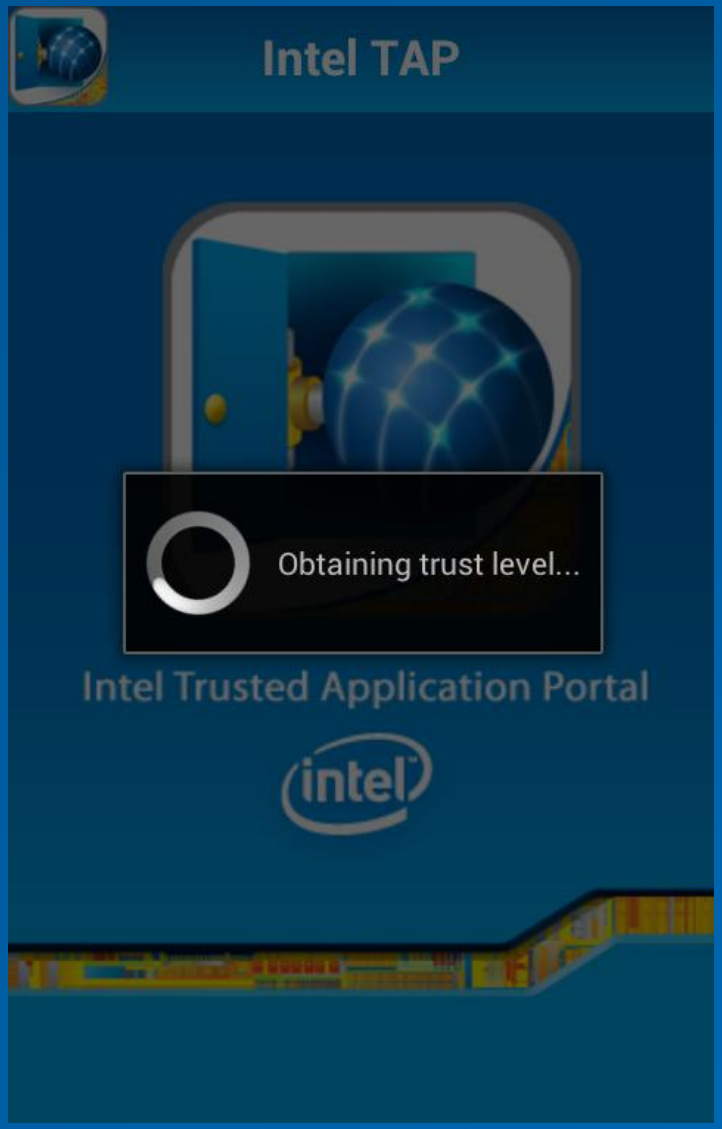
- Keeping us legal
- Availability of information
- Protection of information
- Industry influence
- Cost effectiveness of controls

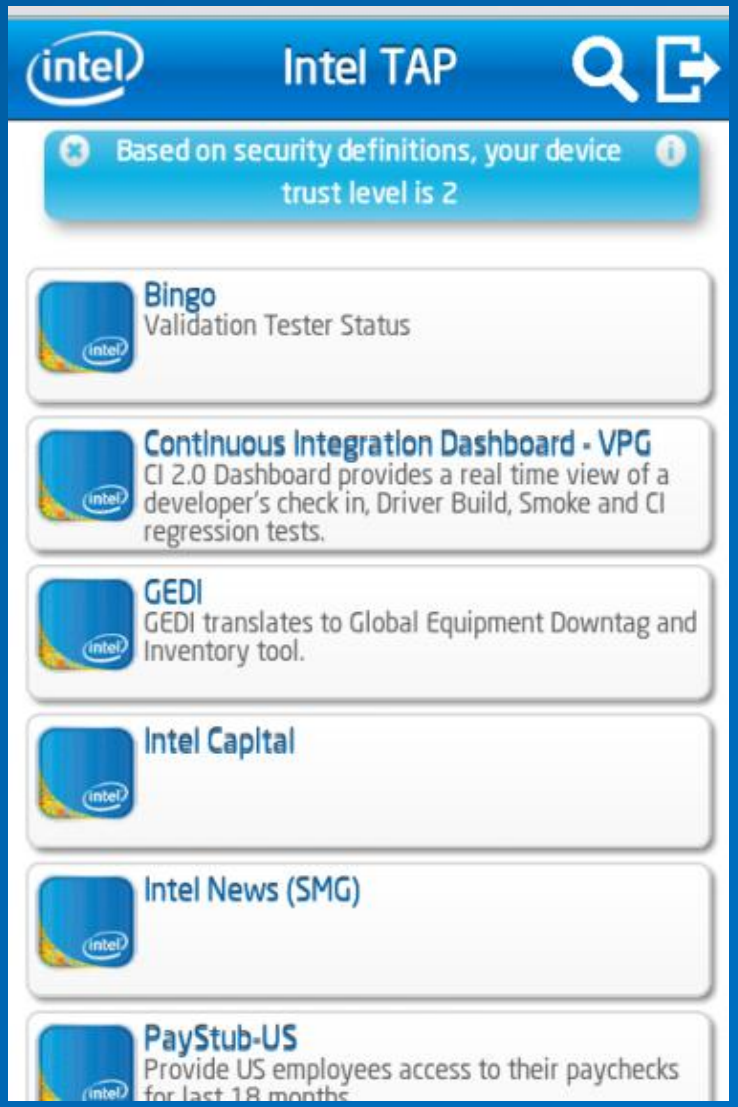


Locked Down
Information assets should be **fully** protected

Our Mission is to Protect to Enable

DEMO





How does it work

- User launches the TAP client application
- TAP client application performs the trust calculation
- TAP client application triggers an API to the McAfee* Pledge OTP
  - User confirms the generation of the OTP
- The One-Time-Password being validated on the Gateway
- Gateway requests Kerberos ticket on user's behalf
- Backend web application is being accessed.

Components

Components – cont.

- TAP client application
  - A lightweight client application
  - Responsible for the client trust calculation
- Application gateway and authentication layer.
  - Resides in the enterprise demilitarized zone (DMZ)
  - provides the layer of enforcement by filtering the access
- Trust broker
  - Calculates and responds with the trust level decision
  - Contains the business logic and the granular trust level

Scenario A: BYO Smartphone

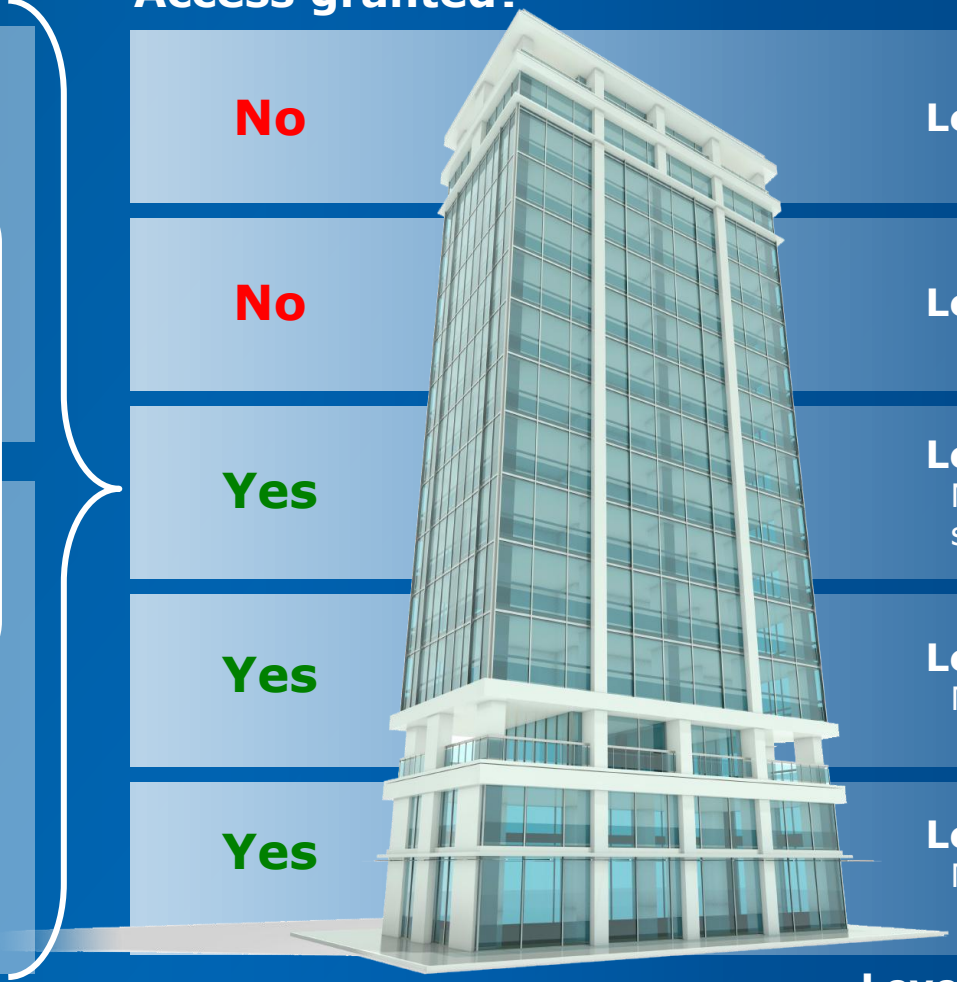
Joe has a personally owned smartphone. He is in a coffee shop.

Trust Level	Access granted?	Access Level
Device Trust Level = 2	No	Level 5: Top Secret
Smartphone + Coffee Shop	No	Level 4: Top Secret
	No	Level 3: Restricted Secret
	Yes	**Level 2: Confidential** Remote display of confidential data but no local content storage
Authentication Method = user OTP plus PIN	Yes	**Level 1: Unclassified** Container based apps
		Level 0: Internet access only

Scenario B: Intel-managed BYO smartphone

Bob's BYO smartphone has an approved MDM solution installed and is running most current version of OS. OS has "defined" features. Bob is in an airport.

Trust Level	Access granted?	Access Level
Device Trust Level = 3 BYO Smartphone with MDM + Airport Authentication Method = device PIN plus embedded certificate	No	**Level 5: Top Secret**
	No	**Level 4: Top Secret**
	Yes	**Level 3: Restricted Secret** Mostly container-based apps; some native apps by exception
	Yes	**Level 2: Confidential** Native apps
	Yes	**Level 1**: Unclassified Native apps
		Level 0: Internet access only



Trust Calculation

- Dynamically determine what information is accessible based on several factors:
  - User identity
  - Type of device
  - Security controls
  - Physical location (on or off site)
- allow access, deny access, or allow limited or mitigated access
  - Can deny change permissions on certain content
  - Allow view-only permissions
  - Block a download

McAfee* Pledge One-Time-Password authentication

- Using McAfee* Pledge One-Time-Password
- API to generate OTP from the client application
- User experience – no need to enter a password

Single Sign On using Kerberos

- The Gateway authenticates the user
- The Gateway requests a Kerberos ticket on the user's behalf
- The Gateway presents the Kerberos Ticket to the backend web application

Benefits:

- No passwords being transferred, only the Kerberos ticket
- Removes the need for Active Directory credentials on BYOD
- Single Sign On – login once, access multiple times

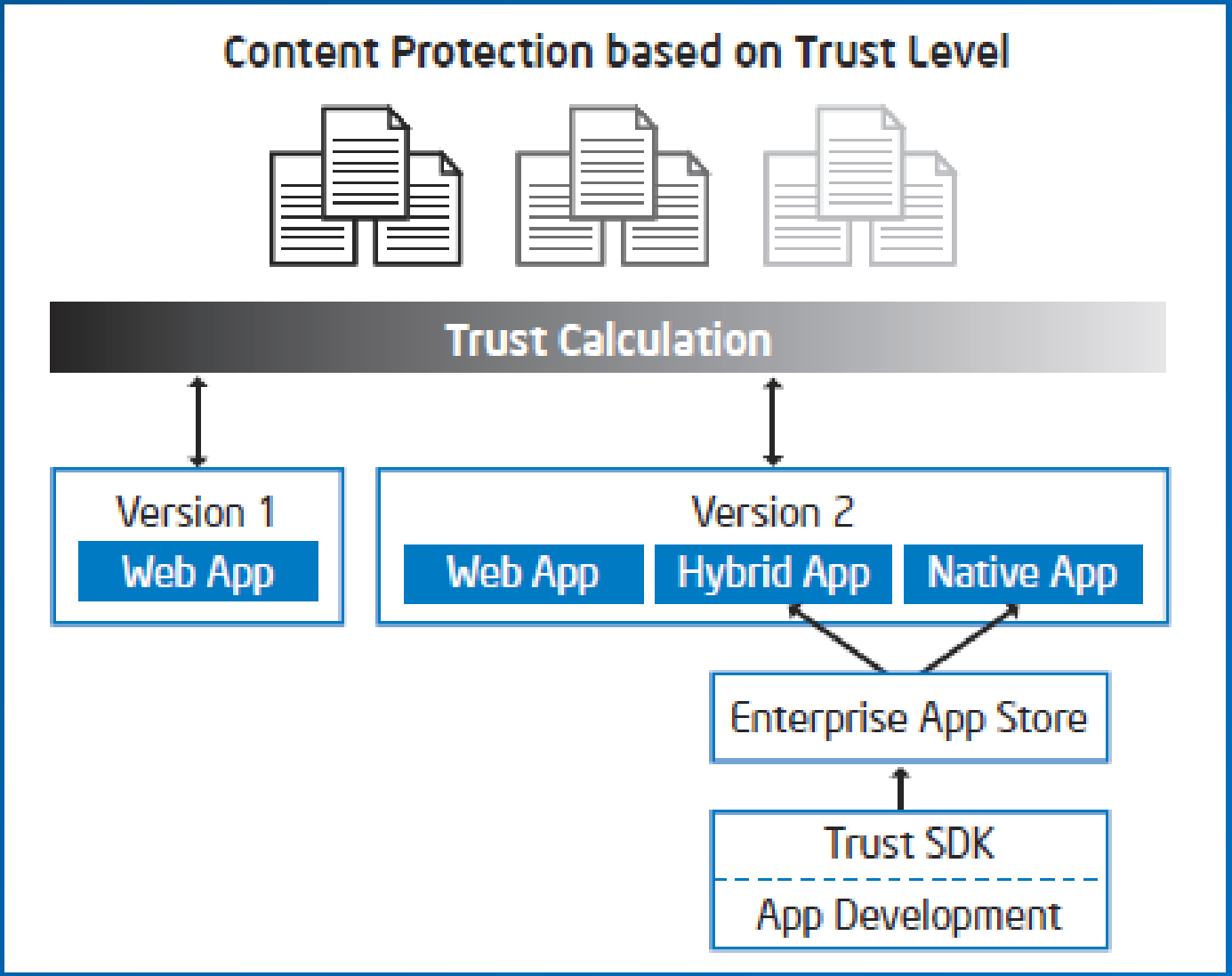
User Experience

- our Trusted Application Portal (TAP) is customizable using scripts and HTML5 to support most SFF devices.
- adheres to the guidelines and standards for human factors engineering.

Results

- > 25 enterprise web applications,
  Smart phones friendly
- > 15 device types, multiple Operating Systems
- > 10,000 installs (35% of BYOD total devices)
- >12,000 accesses to backend applications per week

Next Steps

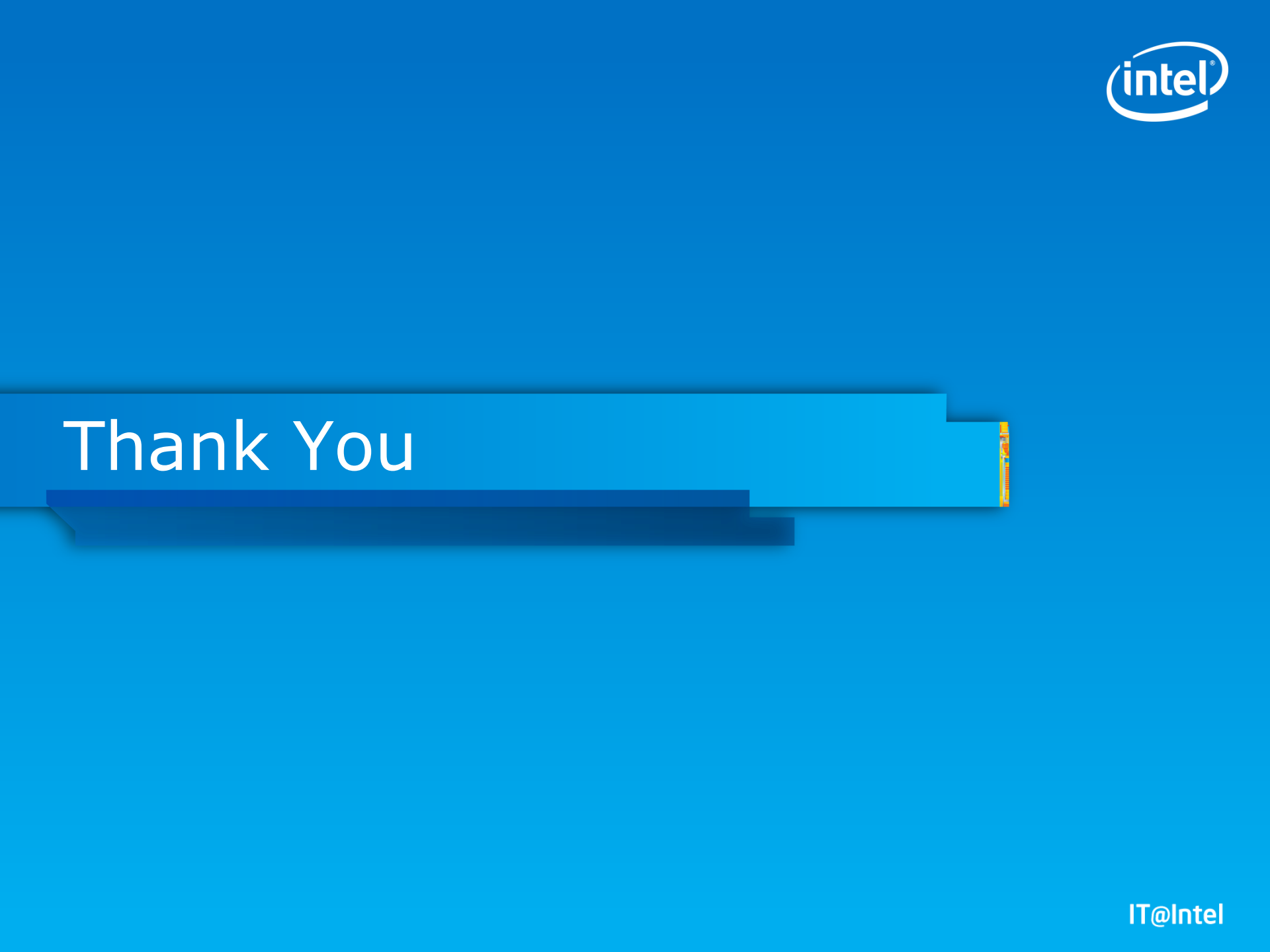


Key Messages

Rethink information security in light of new technologies and attack trends

Capitalize on the opportunity to reduce risk while enabling new technologies

No silver bullet – security still requires “defense in depth”


Thank You
IT@Intel

Additional Resources

[Information Security Protect to Enable Strategy video]

[Rethinking Information Security]

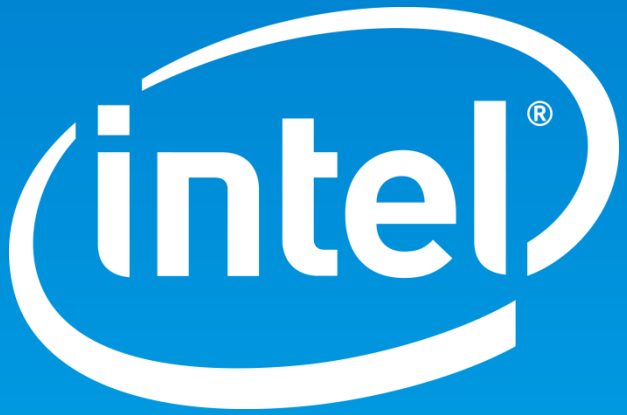
[Intel IT's Security Business Intelligence Architecture]

[Granular Trust Model Improves Enterprise Security]

Learn more about Intel IT's Initiatives at [Intel.com/IT]

IT@Intel Sharing Intel IT Best Practices with the World

Learn more about Intel IT's Initiatives at www.intel.com/IT


intel