

Fear and Loathing in BYOD

or

"What I Learned Reading the SANS Mobility Survey Results"

Sponsored by GIAC and
Trusted Computing Group

© 2013 The SANS™ Institute – www.sans.org

Today's Speakers

- Joshua Wright, SANS Analyst and Senior Instructor
- Lisa Lorenzin, Principal Solutions Architect, Juniper Networks
- Courtney Imbert, Technical Director, GIAC

© 2013 The SANS™ Institute – www.sans.org

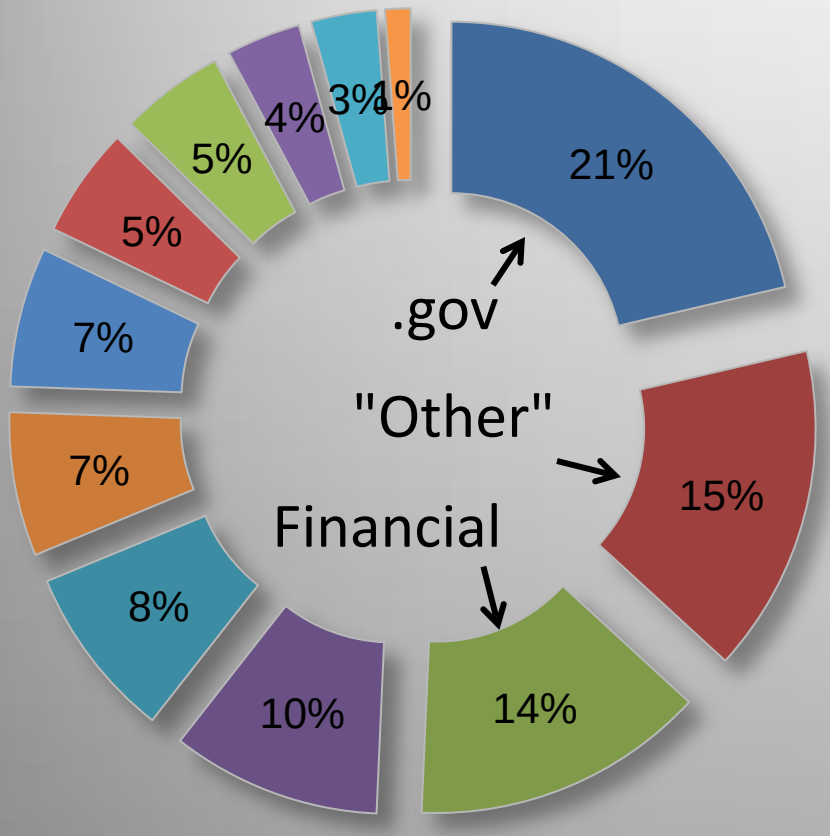
SANS Market Analysis Survey

- SANS conducted a survey on Bring Your Own Device policies and practices
- Nearly 600 respondents, Oct. and Nov. 2013
- The results are…not inspiring

Vulnerabilities and attacks against mobile are expanding. Demand continues to increase. Defense policies and practices…stagnate?

© 2013 The SANS™ Institute – www.sans.org

Who Participated?



- Well-distributed survey participation
- Ample representation from many groups
- Roughly even split across large, medium, and small organizations
- 39% represent international organizations

© 2013 The SANS™ Institute – www.sans.org

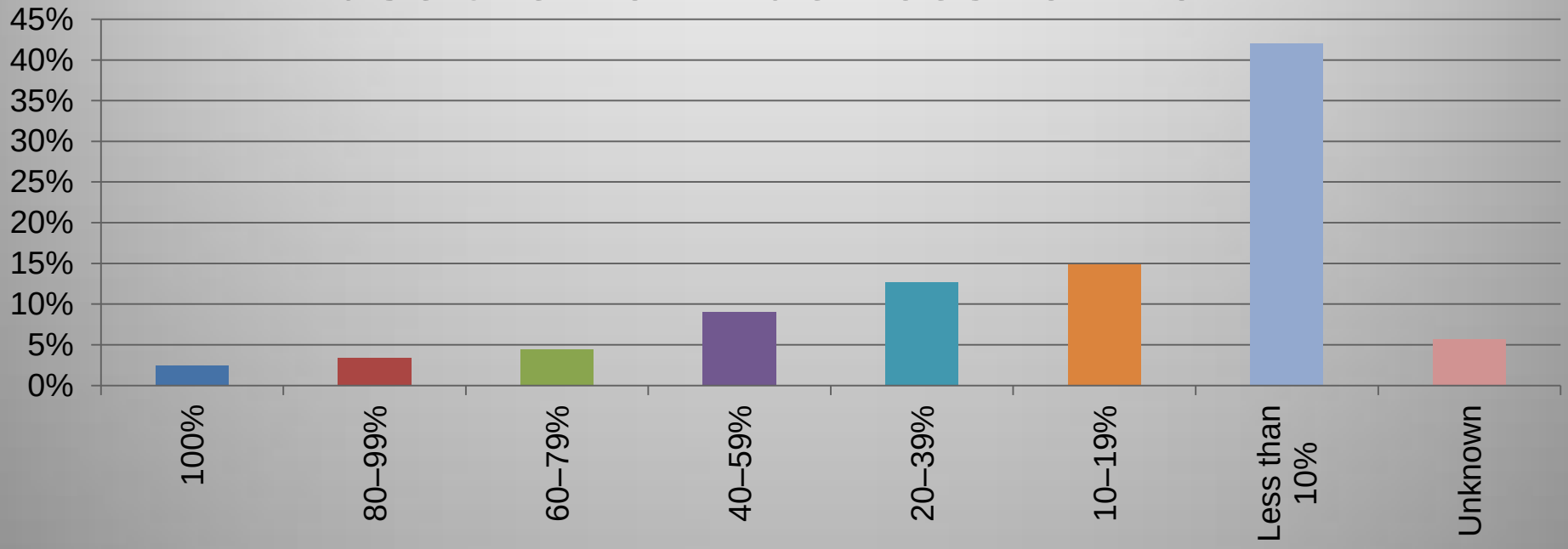
Roles and Responsibilities

- 47% of respondents were at the management, director, or executive level
- Of the remaining respondents, varied technical roles
  - Network and system ops
  - Security analysts
  - Risk/policy/compliance
- Mostly staff employees, few consultants

© 2013 The SANS™ Institute – www.sans.org

BYOD Use

What percent of your workforce currently use their own devices for work?



Respondents indicated that less than 20% of their organizations' employees use personally owned devices for work.

© 2013 The SANS™ Institute – www.sans.org

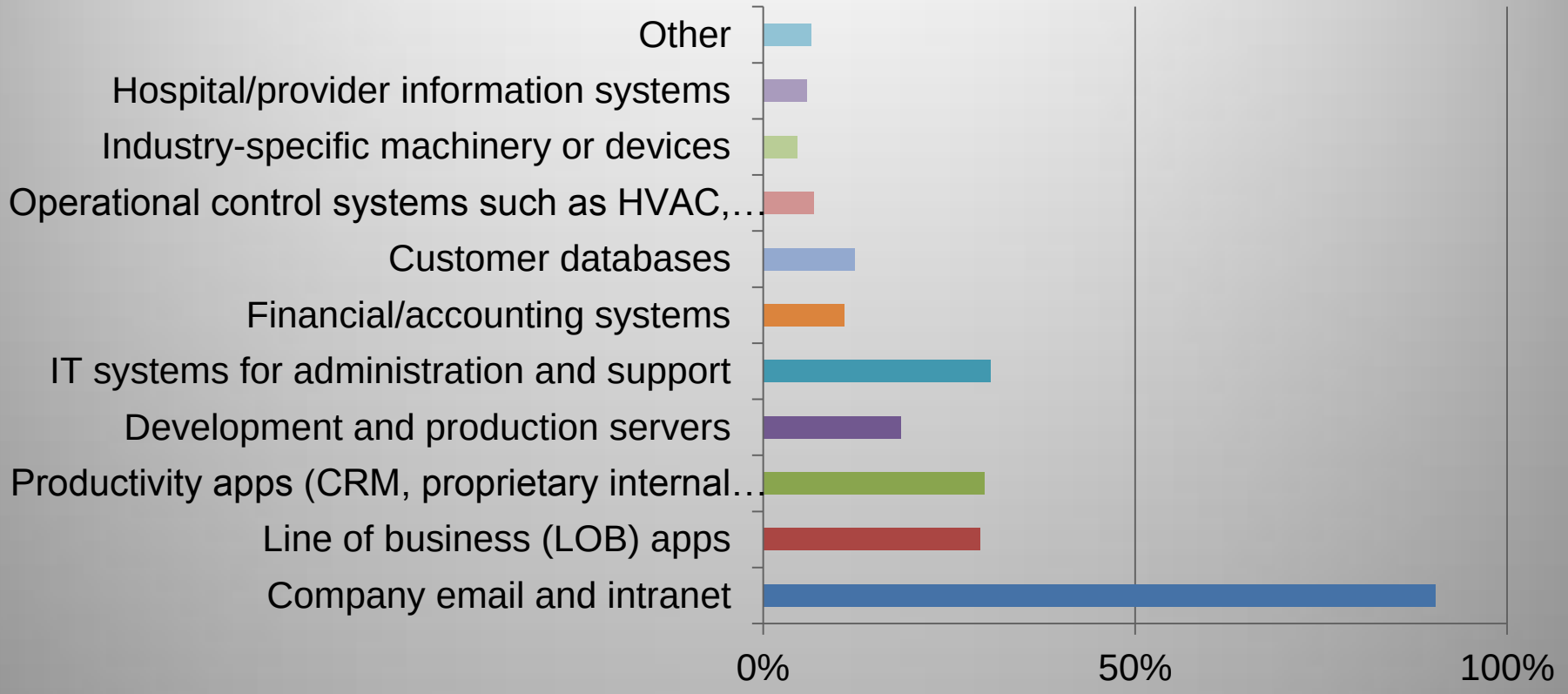
Wait, What?

- These numbers are up, 10% from last year's survey (still seems low)
- Gartner predicts 85% of companies will use BYOD by 2017, 50% to require its use!
- Some possibilities:
  - Respondents hate BYOD and are lying
  - Users are using BYOD without IT knowledge
  - Gartner is wrong…no, that can't be right

[1] http://www.pcworld.com/article/2036980/half-of-companies-will-require-byod-by-2017-gartner-says.html

© 2013 The SANS™ Institute – www.sans.org

Application Use

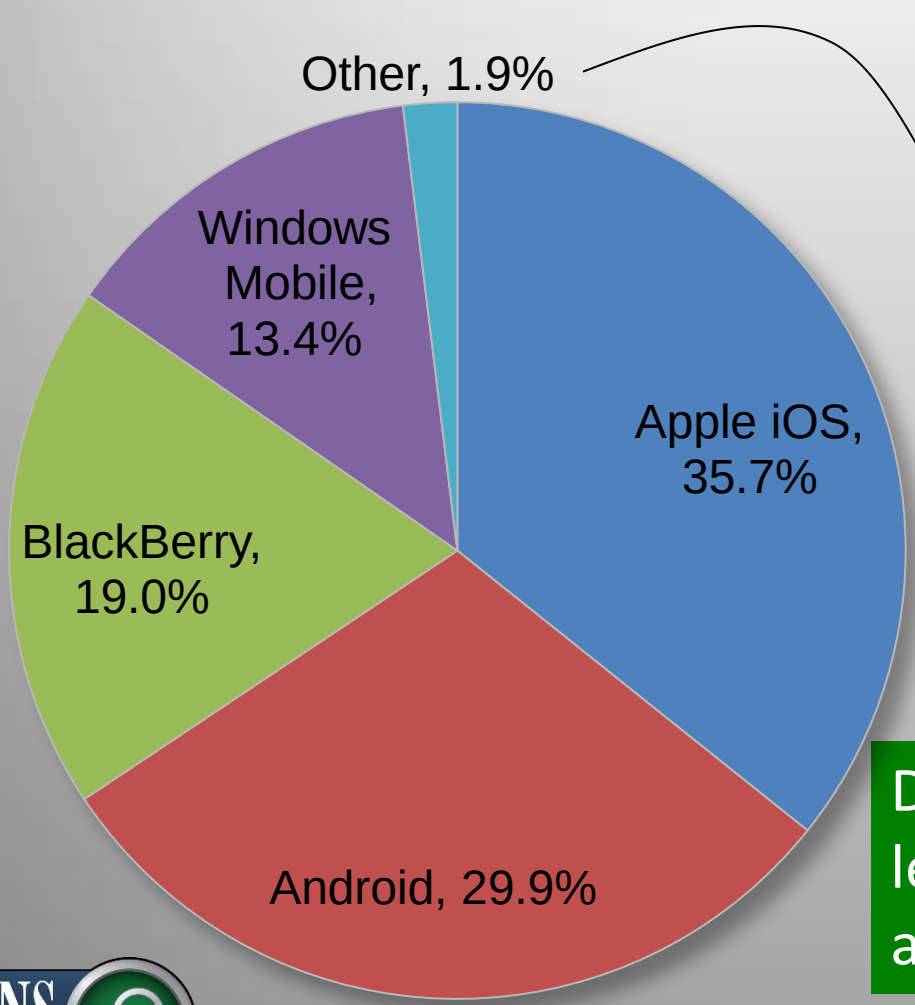


Email remains king for BYOD enterprise data use, but ERP/CRM/LOB apps are growing. It's OK to freak out now.

© 2013 The SANS™ Institute – www.sans.org

Platform Use

"What operating systems is your workforce using to access these resources? Select all that apply."





Despite Android's worldwide lead, iOS leads in enterprise adoption among respondents.

© 2013 The SANS™ Institute – www.sans.org

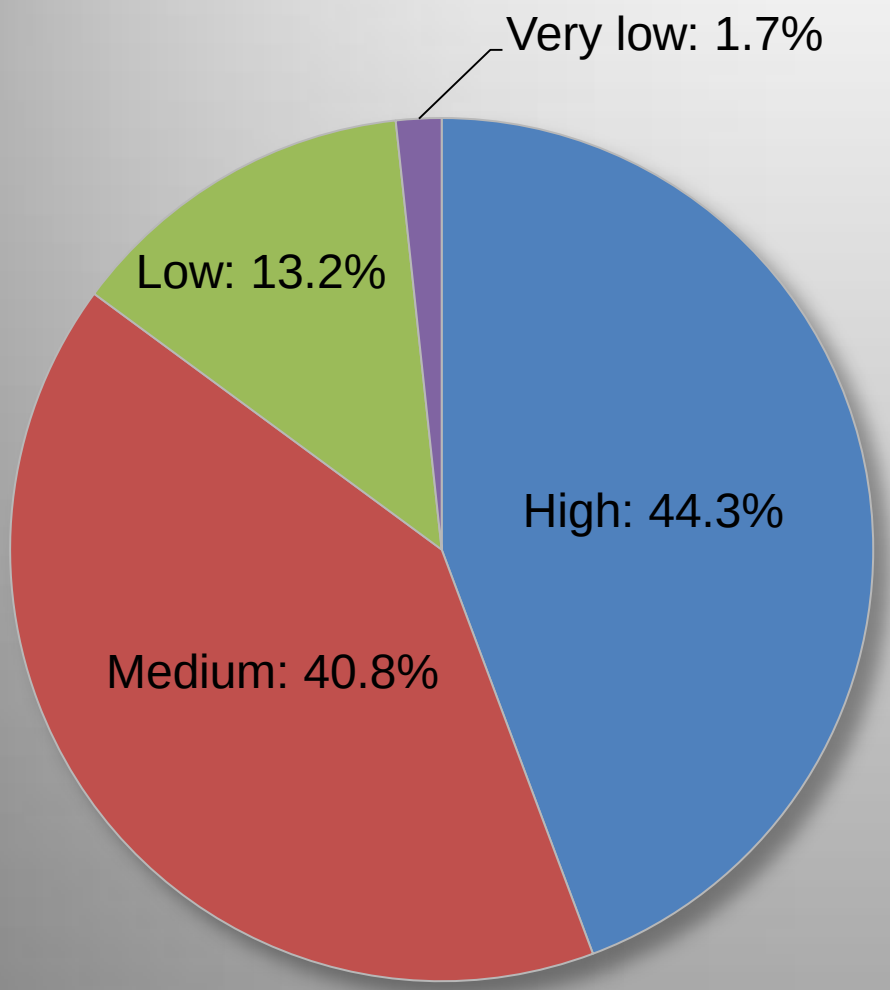
So Far, So Good

Of these results, no tremendous surprises so far…

…but here's where things get weird.

© 2013 The SANS™ Institute – www.sans.org

BYOD Perception of Risk

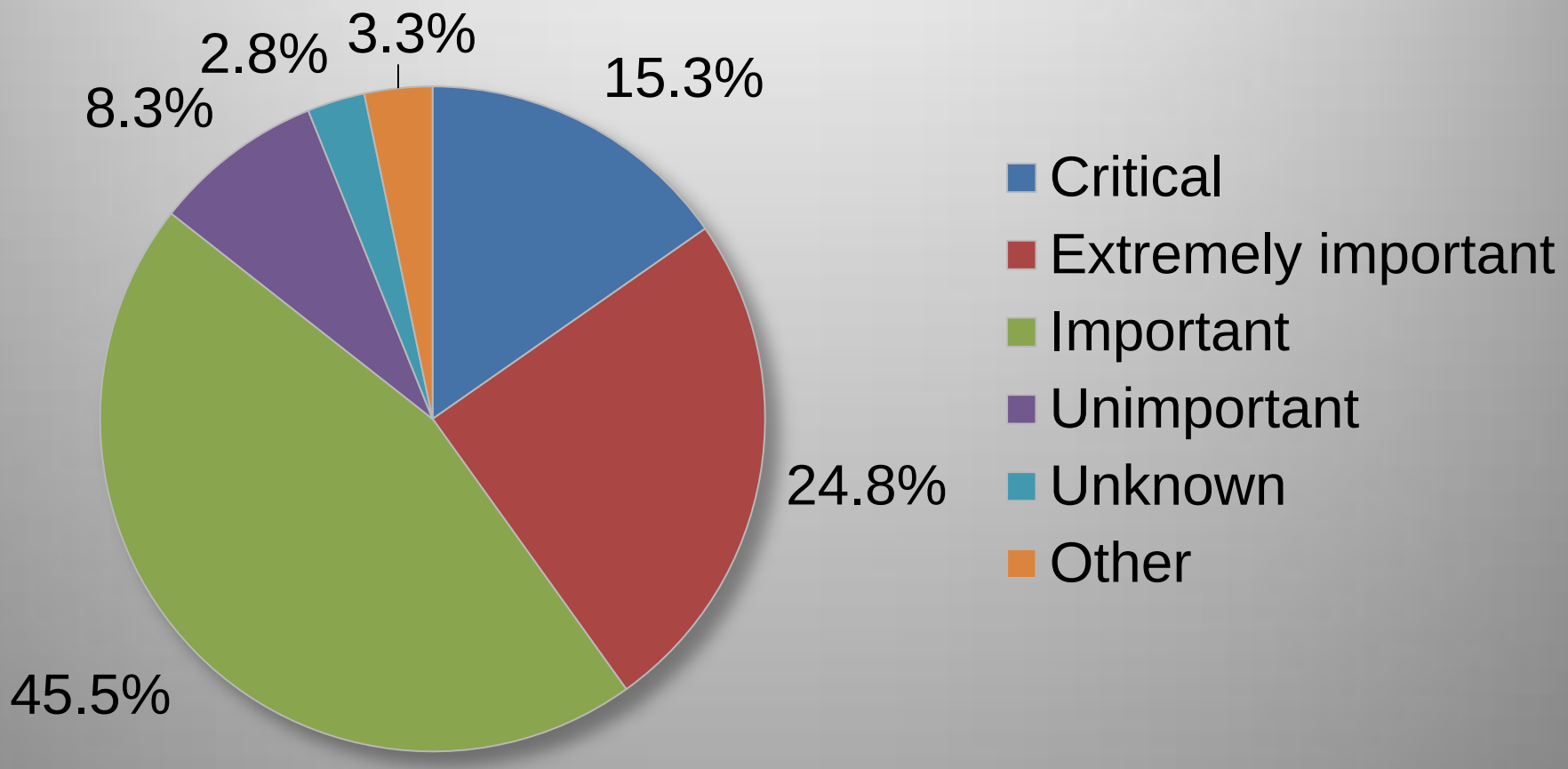


85% of respondents are Somewhat or Very Concerned about BYOD's risks

Insufficient controls, lack of manageability and visibility, mobile malware, legal issues, and user mistakes widely seen as concerns.

© 2013 The SANS™ Institute – www.sans.org

Organizations are Committed to BYOD Deployment



© 2013 The SANS™ Institute – www.sans.org

Yet…

- 36% of organizations rely solely on user education to mitigate mobile device threats
- 35% of organizations have "no protection against hostile applications" on BYOD devices
- The primary security technique used to protect data access for mobile devices is:

VPN

© 2013 The SANS™ Institute – www.sans.org

I Heart VPN

- VPN is a great technology
  - Integrity and confidentiality for data transit
- Many organizations use VPN for an authentication layer
- However, VPN does not solve the security challenges of mobile devices
- Sophisticated platform controls are needed

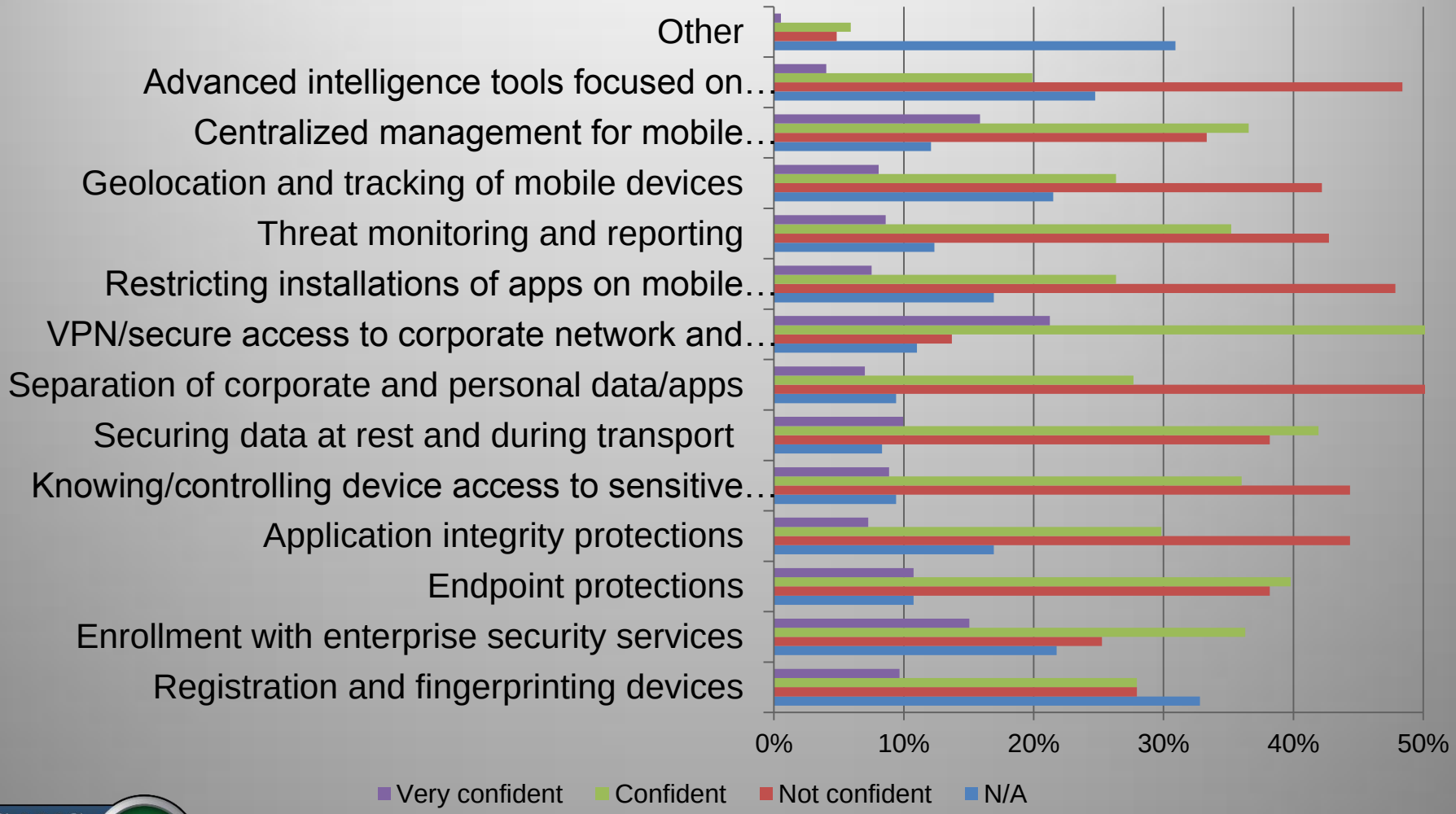
© 2013 The SANS™ Institute – www.sans.org

MDM, MAM, Data Isolation

- Few respondents are using MDM, MAM, or Data Isolation (e.g., Citrix) for data protection
- Part of this is cost and use cases
  - If email is the primary mobile app, perhaps additional data controls are not needed
- As enterprise apps continue to be deployed to BYOD, VPN will not be sufficient

© 2013 The SANS™ Institute – www.sans.org

Red: Not Confident



© 2013 The SANS™ Institute – www.sans.org

Growth and Maturity Are Needed

- Enterprises are not widely adopting sophisticated security controls for mobile
- Cost, lack of flexibility and reliability, lack of resources for deployment, and lack of confidence in controls were cited by respondents

Vendors: Take Note. We need more sophisticated, reliable tools, at a lower cost per device.

© 2013 The SANS™ Institute – www.sans.org

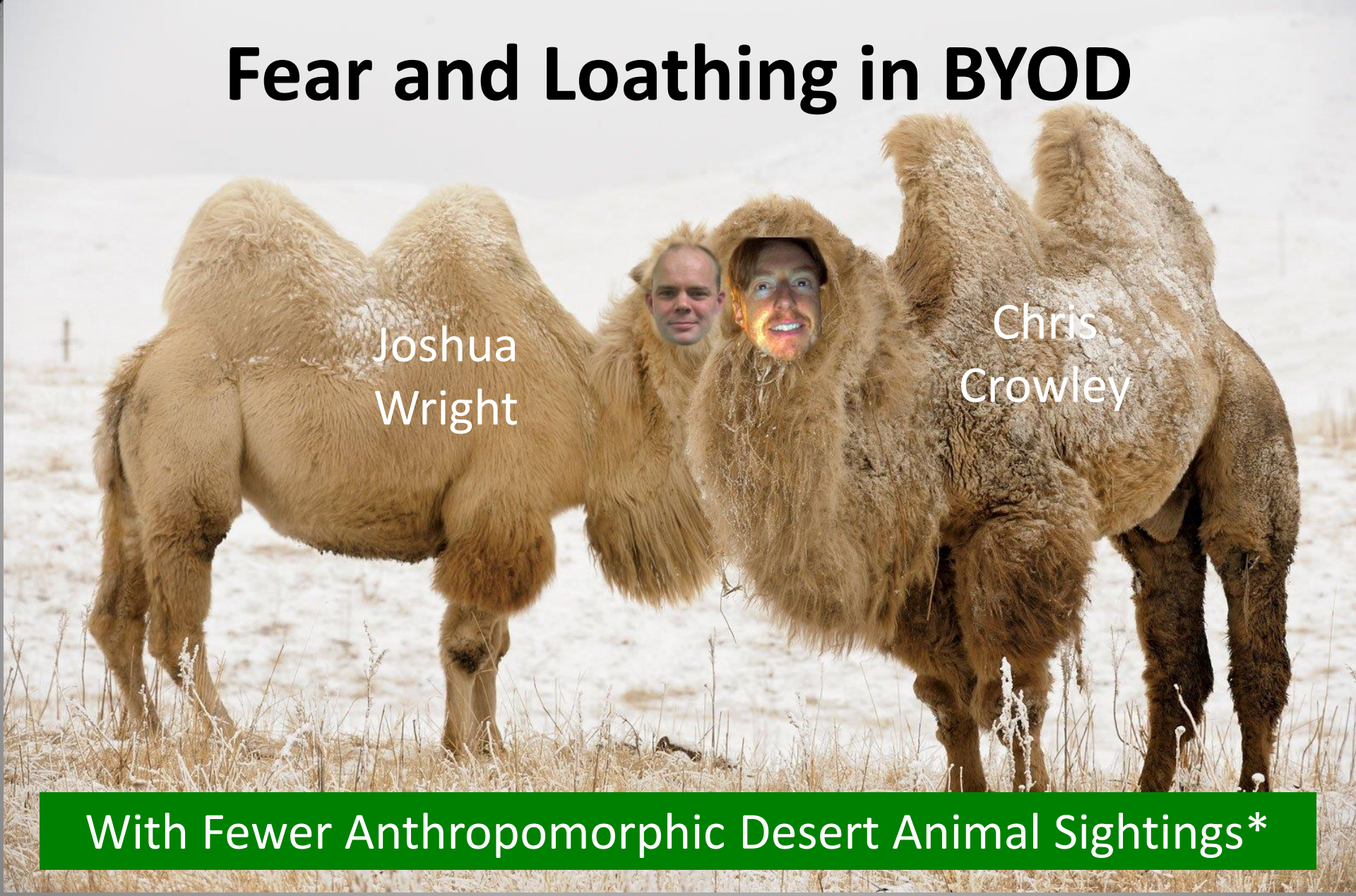
The Result

- Organizations indicate that they are committed to BYOD mobile security…
- …and that the tools for security aren't yet sufficiently baked for widespread adoption…
- …and that, despite concerns, adoption will continue, with growing access to enterprise data

What we get is…

© 2013 The SANS™ Institute – www.sans.org

Fear and Loathing in BYOD



With Fewer Anthropomorphic Desert Animal Sightings*

* I am much better at hacking mobile devices than I am at Photoshop. Really.

© 2013 The SANS™ Institute – www.sans.org

What Organizations Can Do

- Learn to scrutinize mobile applications: You can't evaluate all apps, but you should identify flaws in critical apps prior to adoption
- Adopt MDM systems of some sort, but don't fall in love: be prepared to reevaluate yearly while systems mature
- Develop policies to guide BYOD adoption and use: Don't expect your users to intuitively know about the dangers and expected use behaviors



© 2013 The SANS™ Institute – www.sans.org

Conclusion

- A broad group of IT pros and management responded to our survey
- Much of the results were predictable, but still inspiring
- Organizations need to improve mobile device security posture, but have concerns about today's controls
- While controls mature, organizations can take steps to improve the security of deployments today



© 2013 The SANS™ Institute – www.sans.org

SANS Security 575: Mobile Device Security and Ethical Hacking

- 6-day technical, hands-on course
- In-depth analysis of mobile platforms, security features and limitations
- Learn to evaluate mobile apps for iOS, Android through network analysis, reverse engineering, and app manipulation
- Use wireless, network, web hacking techniques to exploit mobile devices.

http://www.sans.org/sec575



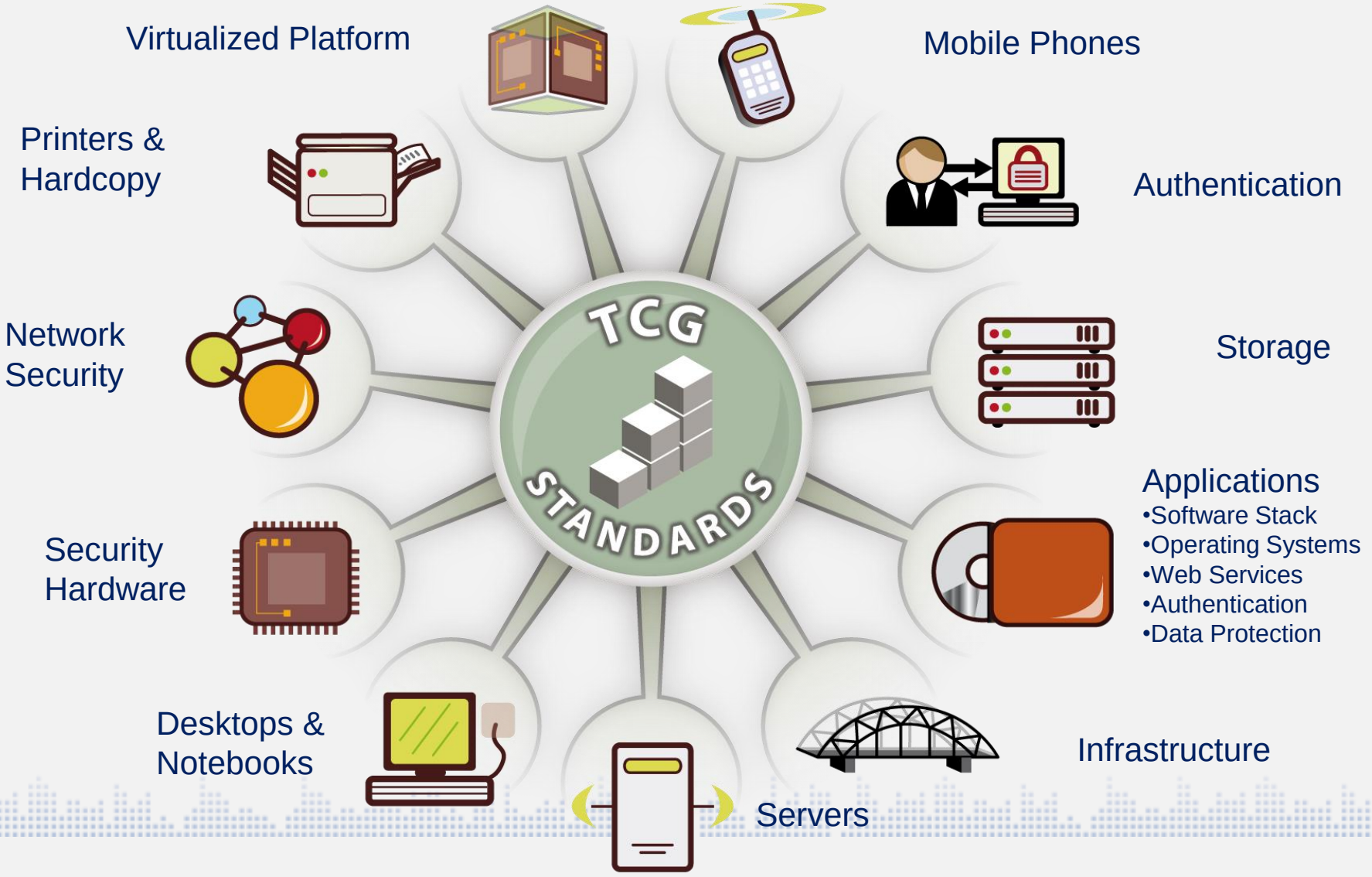
© 2013 The SANS™ Institute – www.sans.org

Using Industry Standards to Cure Fear and Loathing in BYOD Security

Lisa Lorenzin, Juniper Networks and co-chair TCG Trusted Network Connect Work Group

Copyright 2013 Trusted Computing Group

TCG: Standards for Trusted Systems



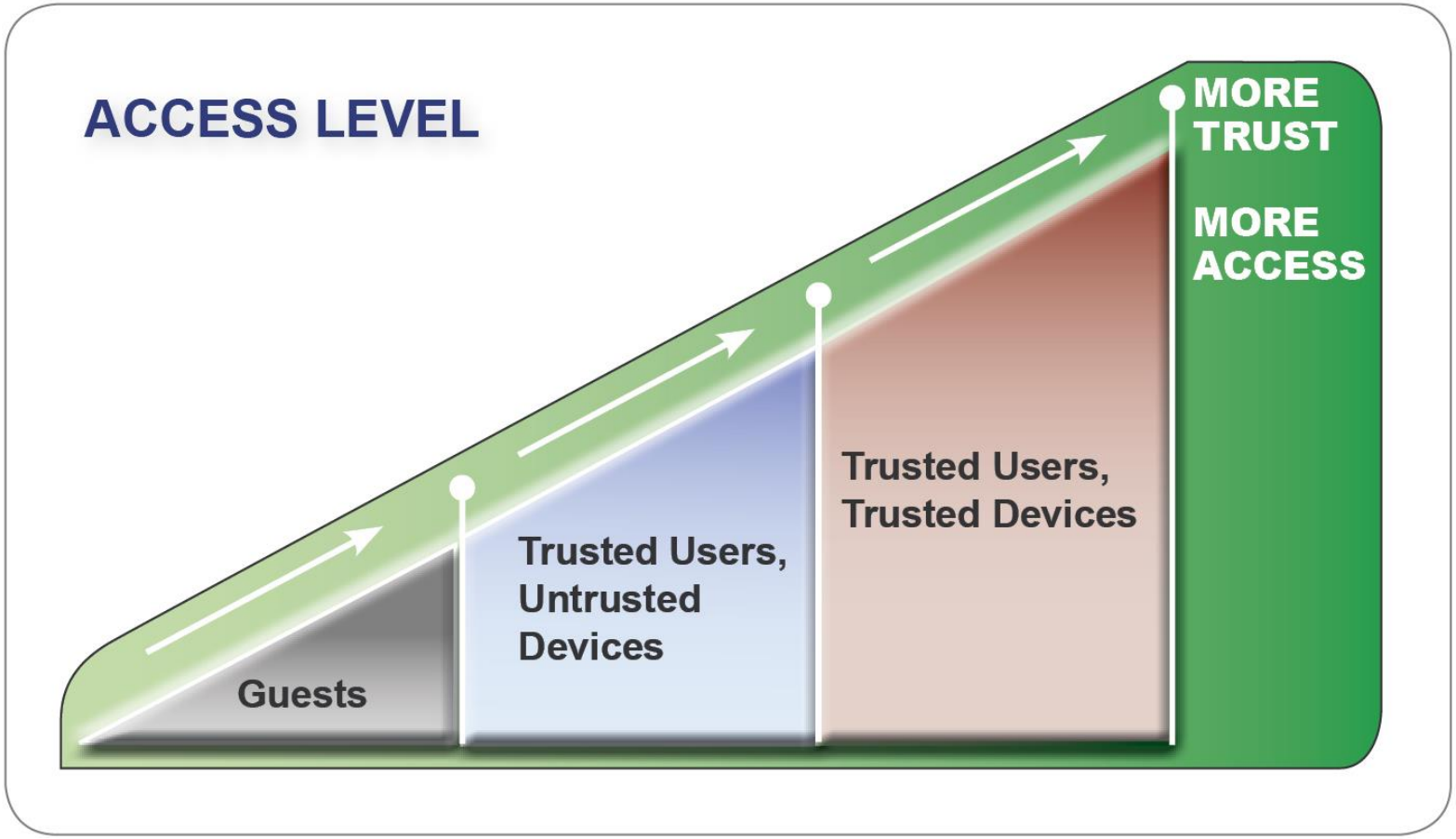
BYOD Security Is Hard…But There's Help

- TCG has already developed security solutions
  - Notebook computers and tablets based on a Trusted Platform Module (TPM)
  - Mobile Trusted Module (MTM) for mobile devices (ex. Windows phones)
  - Self-encrypting Drives (SEDs) for data protection in mobile devices
  - Trusted Network Connect (TNC) specifications for enterprise networks

TRUSTED COMPUTING GROUP™

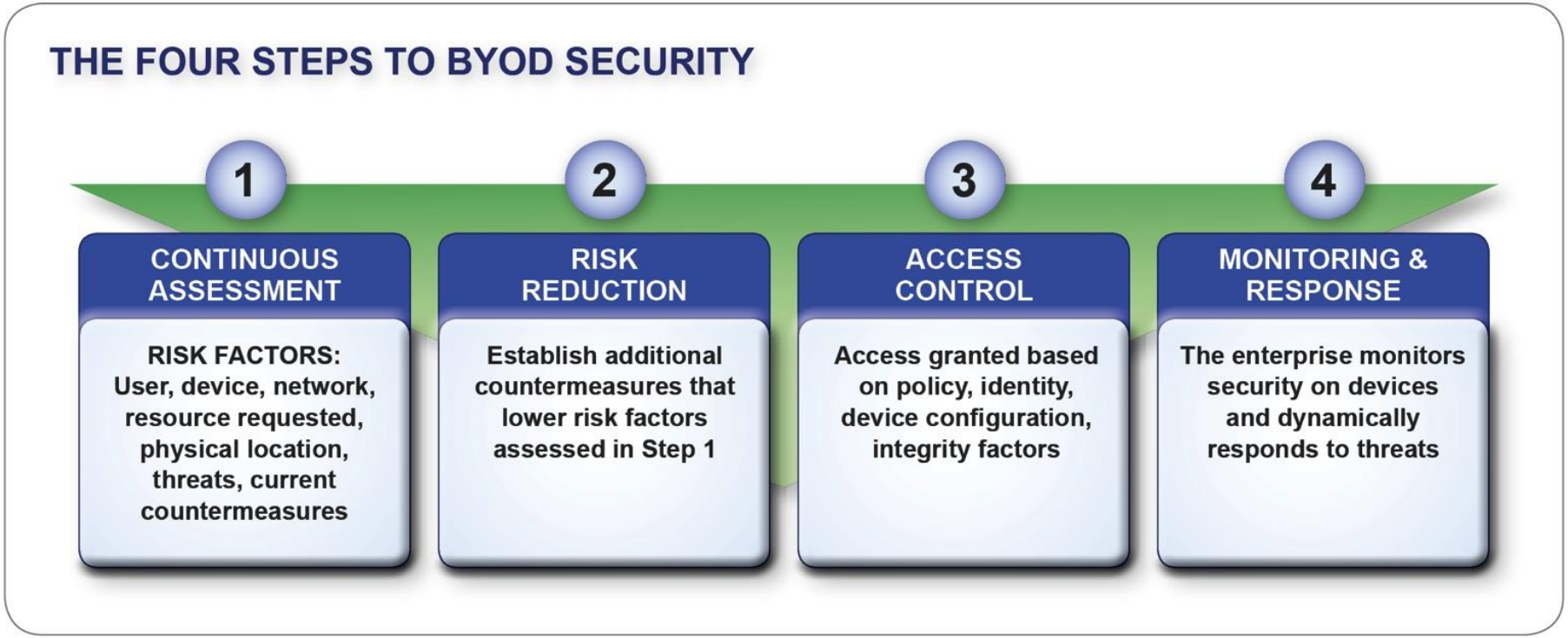
Copyright© 2013 - Trusted Computing Group

Escalating Trust = Increased Access



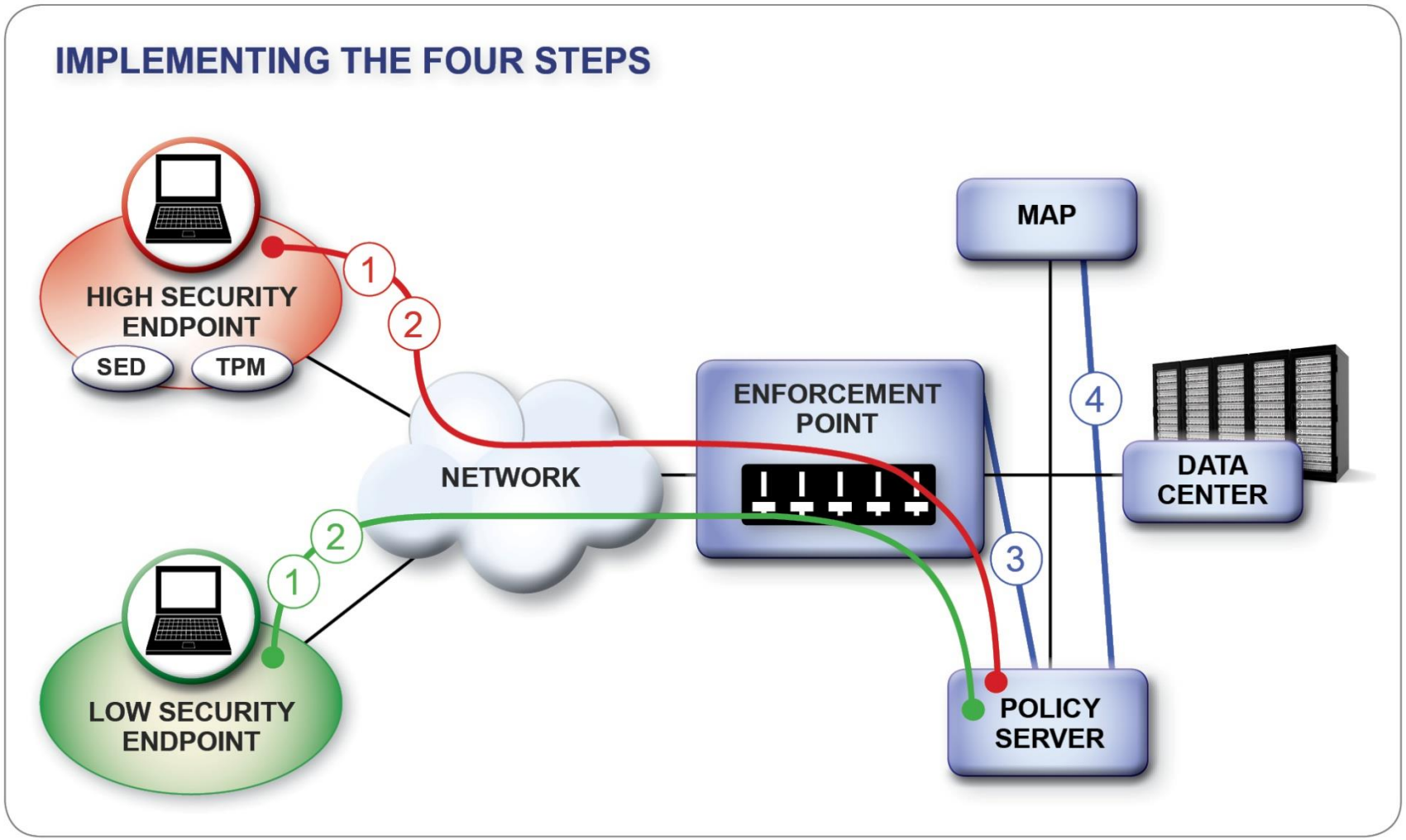
Copyright© 2013 - Trusted Computing Group

Four Steps to BYOD Security



Copyright© 2013 - Trusted Computing Group

Implementing the Four Steps



Copyright© 2013 - Trusted Computing Group

Next Steps and Call to Action

- Read the SANS BYOD survey results white paper
- Read the TCG BYOD security white paper: http://bit.ly/1fGSBPY
- Contact vendors and insist on acquiring TCG-certified technology
- Deploy solutions in pilot first, observe and correct issues, then deploy into production.
- For more information on TCG technologies and architects guides, visit www.trustedcomputinggroup.org

Copyright© 2013 - Trusted Computing Group

GIAC Mobile Device Security Analyst GMOB

- The first vendor-neutral mobile device security certification.
- GMOB candidates must possess a thorough understanding of mobile device penetration testing and the ability to perform a security analysis of mobile applications.
- Includes iOS, Android, Windows and BlackBerry. Learn more and preregister for GMOB at www.giac.org.
- Prepare for the GMOB with SANS SEC575: Mobile Device Security and Ethical Hacking.

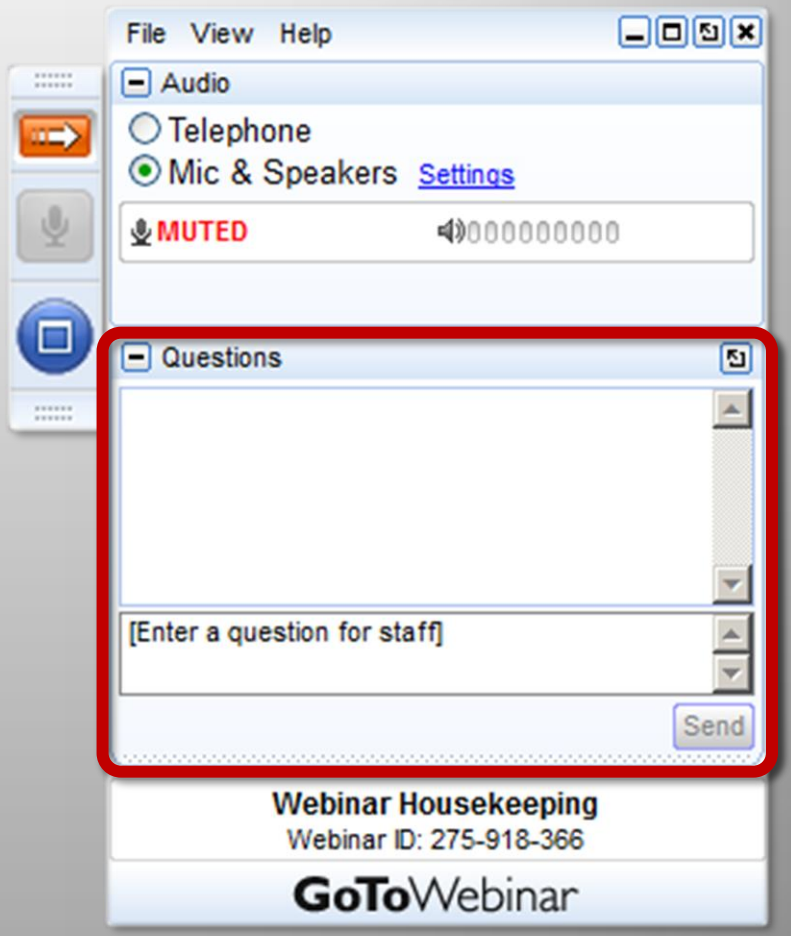


© 2013 The SANS™ Institute – www.sans.org

Q & A

Please use GoToWebinar's Questions tool to submit questions to our panel.

Send to "Organizers" and tell us if it's for a specific panelist.



© 2013 The SANS™ Institute – www.sans.org

Acknowledgements

Thanks to our sponsors:





To our special guests:

Lisa Lorenzin

Courtney Imbert

And to our attendees:

Thank you for joining us today

© 2013 The SANS™ Institute – www.sans.org