

# Security in an Age of Zero Trust

Jon Oberheide  
CTO, Duo Security, Inc.



# Introduction

- Who?
  - Jon Oberheide
  - CTO, Duo Security
  - Reformed(?) hacker, self-loathing academic, person
  - Previously UofM, Arbor, Merit, other MI thingies
- What?
  - Some nonsense^Winsight on security trends
  - WTF is “Zero Trust”?



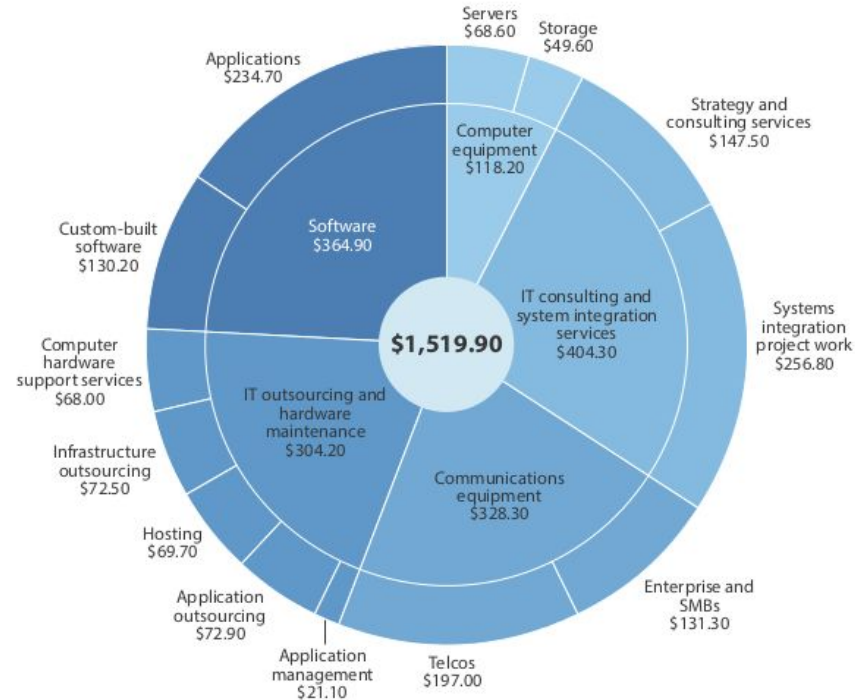
# Not-so-surprising trends

- Cloud

- 1.5 trillion in IT spending
- 2009: 3% implemented, 9% planning
- 2013: 36% implemented, 46% planning

- Mobile

- BYOD: > 286M workers
- > 83% chose their own device



Source: January 3, 2013, "Global Tech Market Outlook 2013 To 2014" Forrester report



# Changes in IT environments

As users go mobile and services go to the cloud, a perimeter-less IT model means a loss of control.



# IT evolution? NO!



# What's new in IT 3.0?

- Users
  - Access from anywhere, anyhow
  - “Zero Trust” environment
- Devices
  - Mobile proliferation
  - BYOD acceptance
- Services
  - Diminishing perimeter
  - IaaS infrastructure, SaaS/cloud apps



# What's new in IT 3.0?

- Users

- Access
- "Zero"

- Device

- Mobile
- BYOD

- Service

- Diminishing
- IaaS infrastructure, SaaS/cloud apps



**HOORAY  
PRODUCTIVITY!**



# What's new in Sec 3.0?

- Users

- Access from anywhere, anyhow ← User-targeted attacks
- "Zero Trust" environment ← Phishing, credential theft, etc

- Devices

- Mobile proliferation ← Emergence of mobile threats
- BYOD acceptance ← Limited endpoint control

- Services

- Diminishing perimeter ← Loss of visibility and control
- IaaS infrastructure, SaaS/cloud apps ← Security by contract

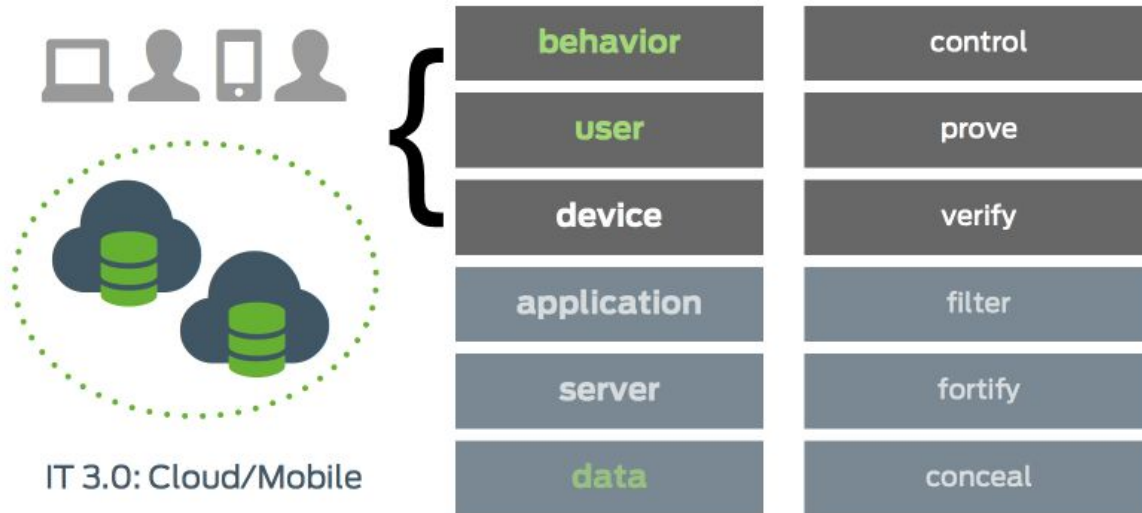




# Security challenges in IT 3.0

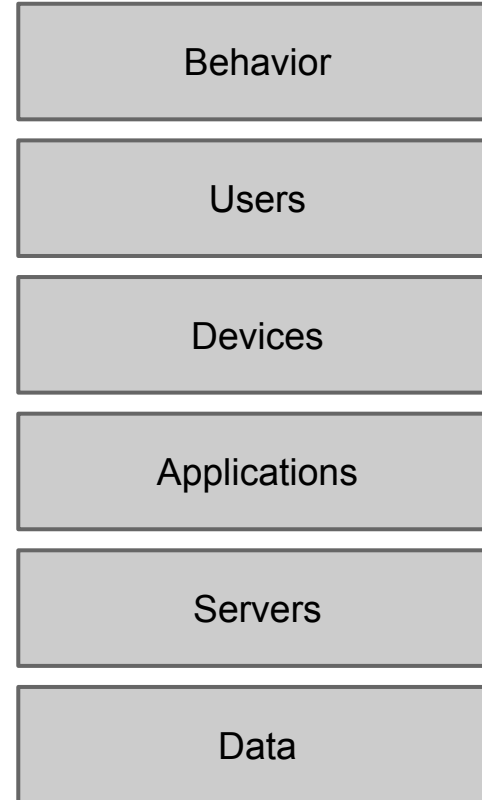
A loss of control precludes the deployment of most traditional security controls in an IT 3.0 environment.

Security must move up the stack, just as attackers have.

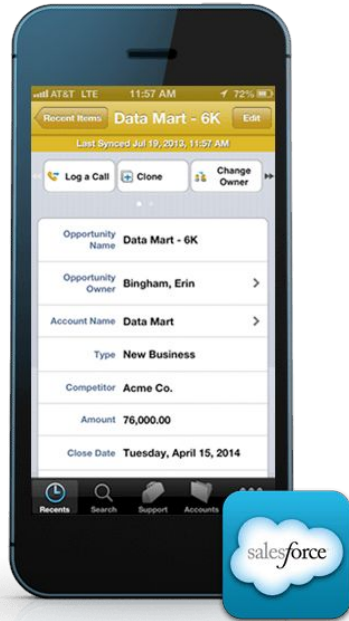


# Where are our current controls?

- AV/HIDS
  - FW/IDS/IPS
  - DLP
  - WAF
  - SIM/SEM
  - DB/DAM
  - Data protection
- 
- The diagram consists of seven arrows originating from the control list on the left and pointing to the system layers on the right. The arrows are as follows: AV/HIDS points to Behavior; FW/IDS/IPS points to Users; DLP points to Devices; WAF points to Applications; SIM/SEM points to Applications; DB/DAM points to Servers; and Data protection points to Data.



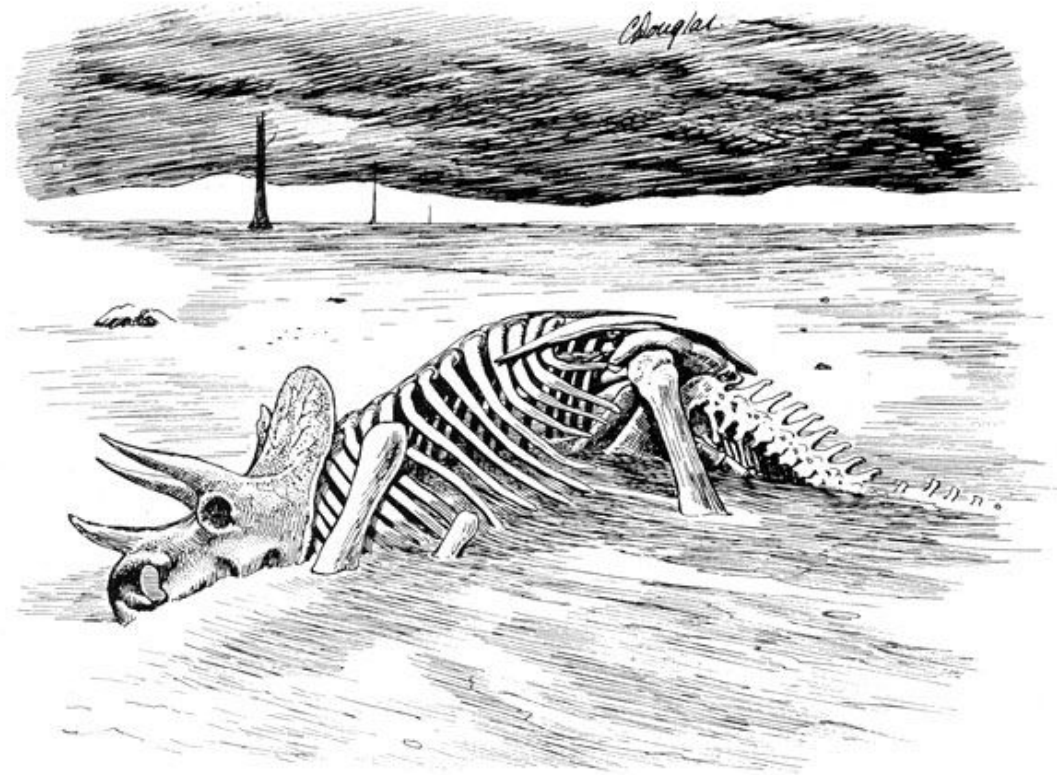
# Case study: Salesforce on mobile



How do you protect this environment?



# It's been a (not-so) good run



# AV is dead?

## RISK ASSESSMENT / SECURITY & HACKTIVISM



### Antivirus pioneer Symantec declares AV “dead” and “doomed to failure”

Company concedes AV fails to catch majority of malicious attacks in circulation.

by Dan Goodin - May 5 2014, 12:25pm

Commercial antivirus pioneer Symantec has declared its software “dead” and “doomed to failure” in a new report. The report, titled “Antivirus is dead? If you think that's news, you've been living in a different world”, states that the growing inability of traditional antivirus software to catch malicious attacks in circulation is a major concern. Symantec, a leading provider of antivirus software, has been a pioneer in the industry for over 30 years. However, the company's latest report suggests that its software is no longer effective in protecting users from malicious attacks. The report states that the growing inability of traditional antivirus software to catch malicious attacks in circulation is a major concern. Symantec, a leading provider of antivirus software, has been a pioneer in the industry for over 30 years. However, the company's latest report suggests that its software is no longer effective in protecting users from malicious attacks. The report states that the growing inability of traditional antivirus software to catch malicious attacks in circulation is a major concern.

Topic: [Security](#)

Follow via:  

# 'Antivirus is dead? If you think that's news, you've been living in a different world'

**Summary:** With the continuing rise of cloud services, security execs have been proclaiming the death of antivirus software. But, according to F-Secure, the security is not so much dead as changed beyond all



What are security  
vendors saying?



# Symantec?

The diagram illustrates a security architecture where data from various sources is stored in a central 'SECURITY BIG DATA STORE'. This store is connected to three main data history tables: 'CONNECTION HISTORY', 'LOGIN HISTORY', and 'EMAIL HISTORY'. Each table has columns for user information, time, and file/status. Below these tables are icons representing a laptop, a server, and an email, with arrows indicating data flow. At the bottom, a server icon is labeled 'ABC Co.'.

**SECURITY BIG DATA STORE**

**CONNECTION HISTORY**

User Name/Username	Destination/Resource/Type	Time	File

**LOGIN HISTORY**

User Name/Username	Destination/Resource/Type	Time	Status

**EMAIL HISTORY**

Sender	Recipients	Attachments	Time

ABC Co.

<http://www.rsaconference.com/videos/125/the-future-of-security>



# HP?



<http://www.rsaconference.com/events/us14/agenda/sessions/1344/stop-looking-for-the-silver-bullet-start-thinking>





# Cisco?



<http://www.rsaconference.com/videos/126/the-new-model-of-security>



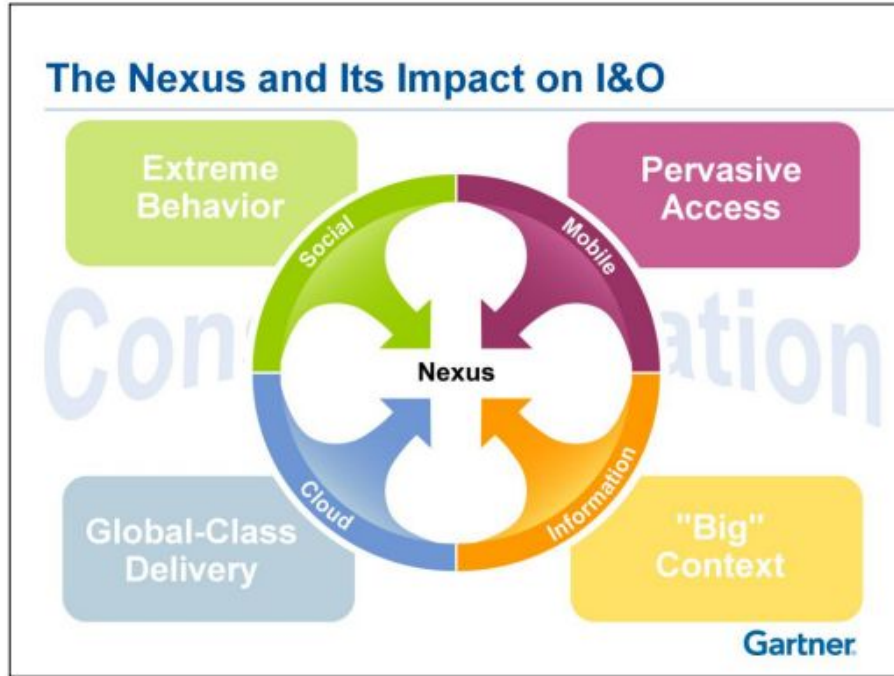
# Qualys?



<http://www.rsaconference.com/videos/127/the-cloud-security-nightmare-or-our-next-great>



# At a high level



- Market speak
- Nexus of forces
- Product positioning
- Vendors at 50k ft altitude



**But I'm afraid of APT!?!**



# APT?



APT?



Actually Pretty Tame



# Not so advanced

- Phishing against HVAC supplier
- HVAC -> Target corporate network
- Default credentials on internal systems
- POS malware written by Russian teenager
- Exfiltration over \_FTP\_



# Who's to blame?

Target, orrrr...the industry?

## COMPLIANCE

### Target, PCI Auditor Trustwave Sued By Banks

Trustwave apparently certified the retailer as PCI compliant -- but can PCI assessors be held liable for data breaches?

The security firm Trustwave and the retailer Target have both been named in a lawsuit filed by a group of banks.

[Home](#) > [Business](#)

### Clean reviews preceded Target's data breach, and others

Article by: [JENNIFER BJORHUS](#), Star Tribune | Updated: March 31, 2014 - 9:27 AM

Critics say company that assessed Target has been sloppy in past



# Who's to blame?

Target, orrrrr...the industry?

COMPLIANCE

## Target, PCI Auditor Trustwave Sued By Banks

Trustwave apparently certified the retailer as PCI compliant -- but can PCI assessors be held liable for data breaches?

The security firm Trustwave and the retailer Target have both been named in a lawsuit filed by a group of banks.

[Home](#) > [Business](#)

## Clean reviews preceded Target's data breach, and others

Article by: [JENNIFER BJORHUS](#), Star Tribune | Updated: March 31, 2014 - 9:27 AM

Critics say company that assessed Target has been sloppy in past

# Who's to blame?

Target, orrrr...the industry?



Adam Greenberg, Reporter

Follow @writingadam

March 13, 2014

## Target did not respond to FireEye security alerts prior to breach, according to report

Share this article:



Target might have been a tad negligent when it came to observing its security systems last year,



# Who's to blame?

Target, orrrrr...the industry?

31

Like

Share

120

Tweet

120

Share



Adam Greenberg, Reporter

Follow @writingadam

March 13, 2014

## Target did not respond to FireEye security alerts prior to breach, according to report

Share this article:



Target might have been a tad negligent when it came to observing its security systems last year,



# Alarming results

- Simple attacks are succeeding at an alarming rate
- Attackers are going after users and their *access*



**What are progressive  
companies doing?**



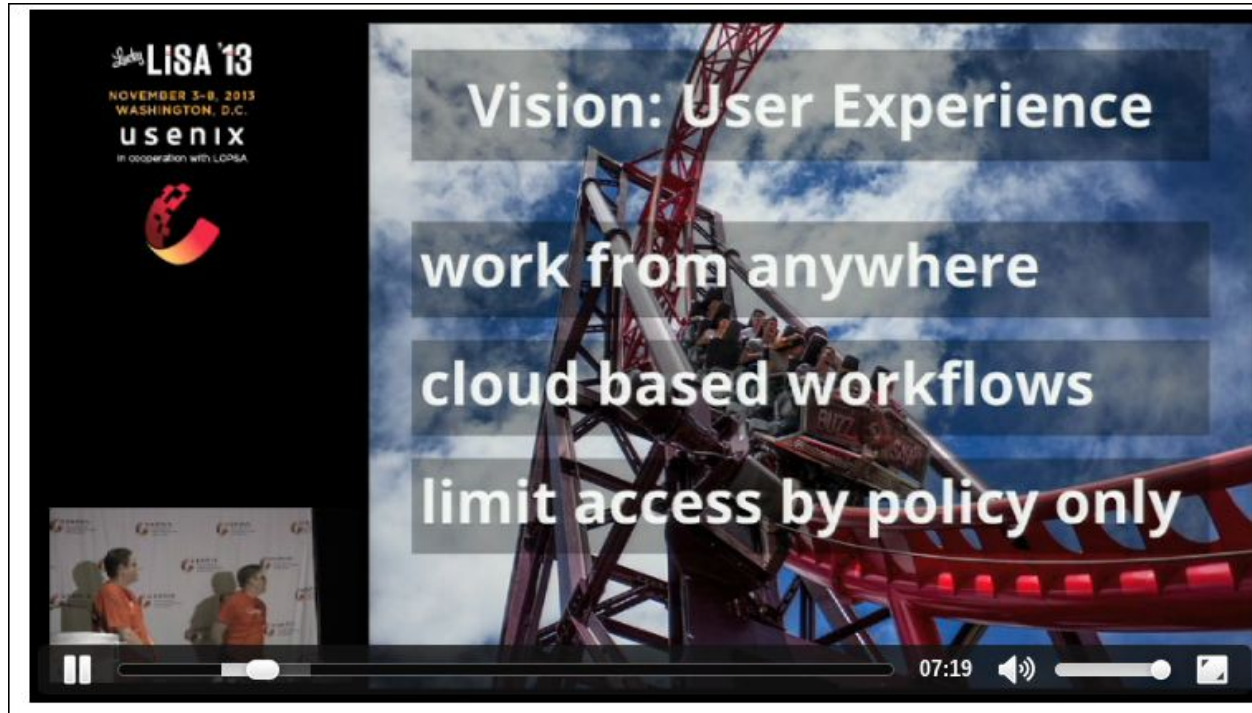
# Google - Beyond Corp



<https://www.usenix.org/conference/lisa13/enterprise-architecture-beyond-perimeter>



# Google - Beyond Corp



<https://www.usenix.org/conference/lisa13/enterprise-architecture-beyond-perimeter>



# Netflix - 100% cloud



<http://www.slideshare.net/mdkail/it-ops-2014-technology-roadmap>

<http://www.amplifypartners.com/interviews/netflix-vp-of-it-on-the-future-of-infrastructure/>

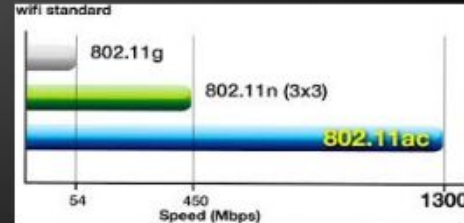




# Netflix - 100% cloud

## Identity Is The New Perimeter

- ZERO TRUST NETWORK ARCHITECTURE
  - CORE NETWORK STABILITY IS PRIORITY #1
  - ARUBA 802.11AC UPGRADE
  - VPN REQUIRED TO DC FROM EVERYWHERE
  - CERTIFICATE-BASED AUTH TO NIGHTMARES
    - EJBCA
    - ARUBA CLEARPASS

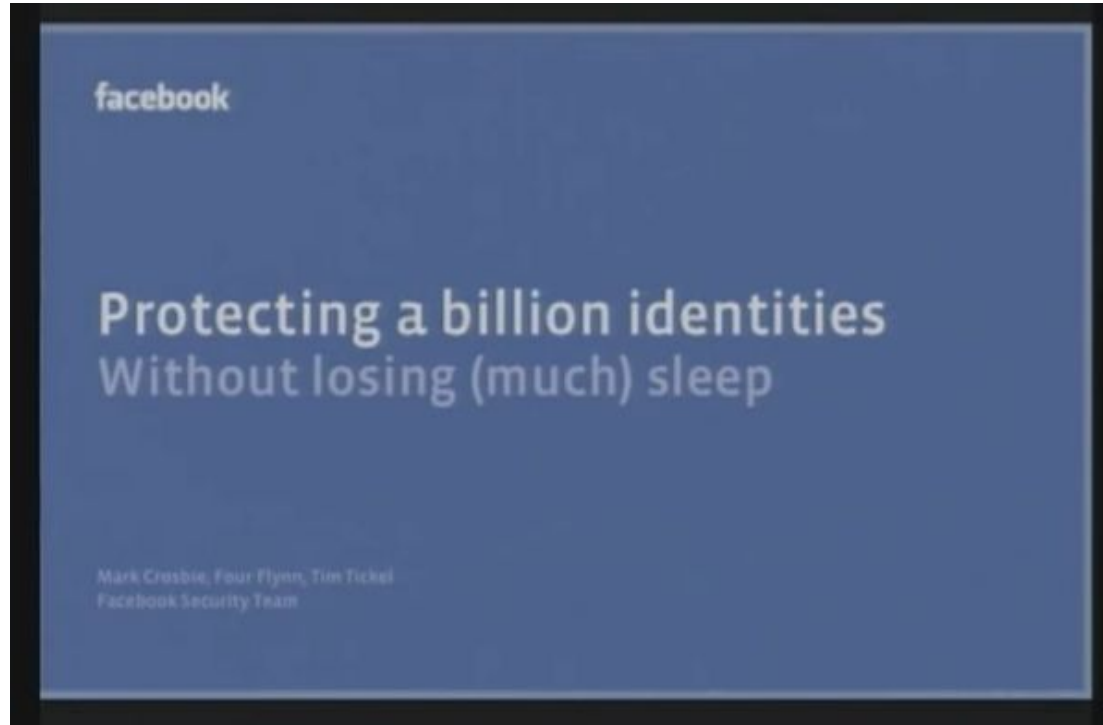


<http://www.slideshare.net/mdkail/it-ops-2014-technology-roadmap>

<http://www.amplifypartners.com/interviews/netflix-vp-of-it-on-the-future-of-infrastructure/>



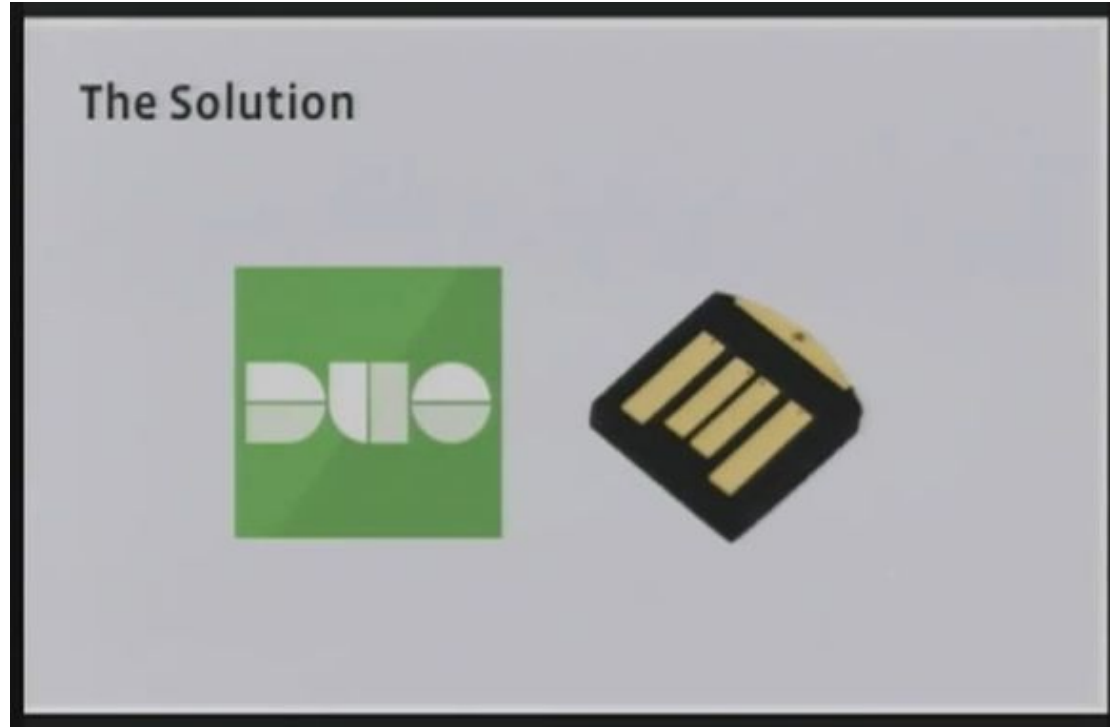
# Facebook - Protect the graph



[http://www.cerias.purdue.edu/news\\_and\\_events/events/security\\_seminar/details/index/d3676r45gc9eir0n1k7u29m0hk](http://www.cerias.purdue.edu/news_and_events/events/security_seminar/details/index/d3676r45gc9eir0n1k7u29m0hk)



# Facebook - Protect the graph



[http://www.cerias.purdue.edu/news\\_and\\_events/events/security\\_seminar/details/index/d3676r45gc9eir0n1k7u29m0hk](http://www.cerias.purdue.edu/news_and_events/events/security_seminar/details/index/d3676r45gc9eir0n1k7u29m0hk)



# Progressive companies

- These companies see the writing on the wall
- Similarities
  - *Embracing* cloud and mobile
  - *Assuming* a zero trust environment
  - *Anchoring* on user and device authentication
  - *Protecting* user access



What should I do?  
I'm not Google,  
Facebook, or Netflix!



# Panic?



Totally valid coping mechanism



# Rejection



“That would never work for my org!”



# Blind acceptance



“I’m burning down my datacenter tomorrow.”





# Keep an open mind

- Digest (breakfast and thoughts)
- Keep an open mind throughout the day
- Watch some of the linked content later
- Think a little further out, beyond the headlines
- Enjoy the conference!



# Questions?

## Q & A

Jon Oberheide

@jonoberheide

jono@duosecurity.com

