

Anti-Spam Mythology: Testing Trumps PR

Joel Snyder
jms@opus1.com
Opus One



Securing Email, Messaging Platforms and Mobile Devices

Agenda

- **What's all this testing nonsense anyway?**
- **Top Myths in Running Enterprise Anti-Spam**

Securing Email, Messaging Platforms and Mobile Devices

Where Did All This Come From?

- **Network World anti-spam tests in Aug/2003 and Dec/2004**
- **First (and only) public test using real message streams**



NETWORKWORLD

RECEIVE AN ELECTRONIC SUBSCRIPTION
CLICK HERE

HOME

RESEARCH CENTERS

- Security
 - Anti-Virus / Spyware / Spam
 - Compliance & Regulation
 - Firewalls / VPN / Intrusion
 - NAC
 - Services
 - Cisco Security Watch
 - Microsoft Security Watch
- LANs & WANs
- VoIP & Convergence
- Network Management
- Wireless & Mobile
- Software
- Data Center
- Small Business Networking
- Cisco Subnet

Security

Whitepapers Guides and Reports Webcasts Podcasts Videos Partner Sites Buy

NetworkWorld.com > Security >

Spam in the Wild, The Sequel

This time, we tested (almost) everyone

[Clear Choice Tests](#) By [Joel Snyder](#), Network World, 12/20/04

[Comments \(1\)](#) [Print article](#)

CLEAR CHOICE TEST

How big can a test get? We found out with our latest in-depth look at the anti-spam industry. Spam is still a huge problem, and there is an equally large market opportunity to fix it.

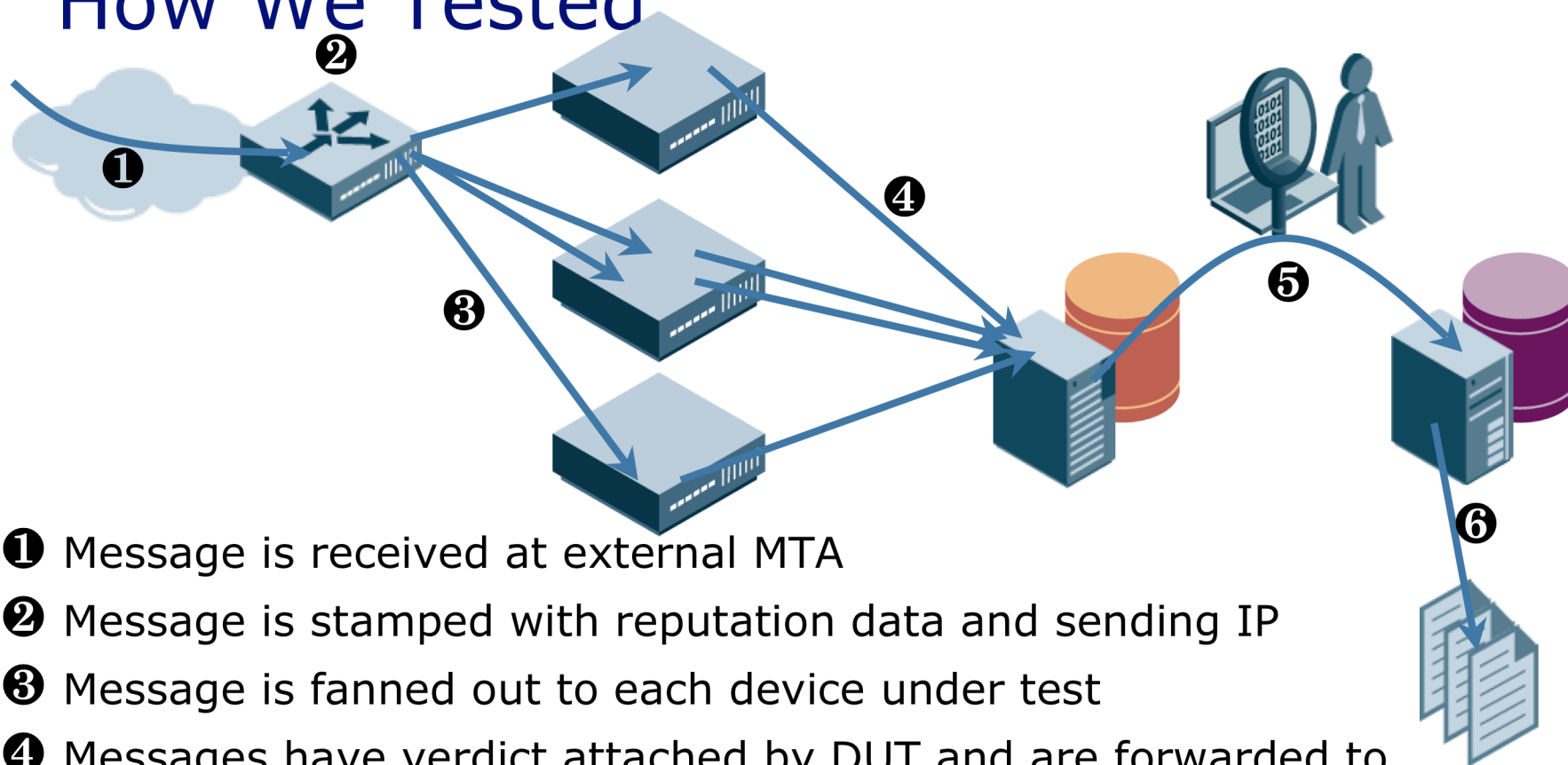
We invited every anti-spam vendor in our [online Buyer's Guide](#) to participate. While we expected to get eight to 10 vendors to sign up, 41 showed up. We tested them all for spam catch rate (including false-positive and false-negative rates), and performance and throughput ([see charts](#)).

Other stories on this topic

- MIT SPAM CONFERENCE
[Tarpits deter impatient spammers](#)
- [Spam pollutes blogs](#)
- [How to fix e-mail authentication spec](#)

Securing Email, Messaging Platforms and Mobile Devices

"How We Tested"



- ❶ Message is received at external MTA
- ❷ Message is stamped with reputation data and sending IP
- ❸ Message is fanned out to each device under test
- ❹ Messages have verdict attached by DUT and are forwarded to mailbox server
- ❺ Master set is combed through by human to classify as spam/not-spam/don't-know; FPs are classified as 1 to 5 by "badness"
- ❻ Many SQL queries later, a report is put together (partially by hand)

Securing Email, Messaging Platforms and Mobile Devices

“When We Tested”

- **Three tests in First Half of 2005**
- **Starting Second Half of 2005, approximately quarterly testing (17 runs as of Feb/2008)**
- **Each test looks at between 15 and 45 scenarios**
- **...and a continuing test plan through 2008**

Securing Email, Messaging Platforms and Mobile Devices

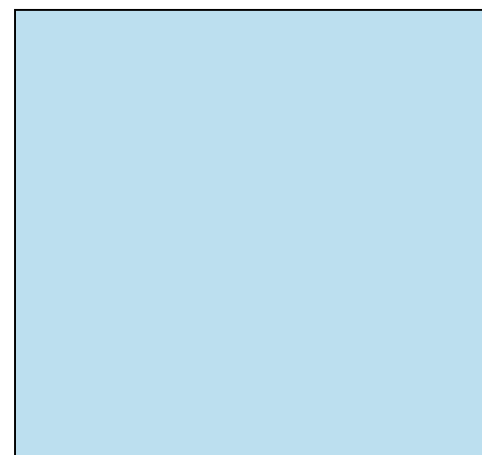
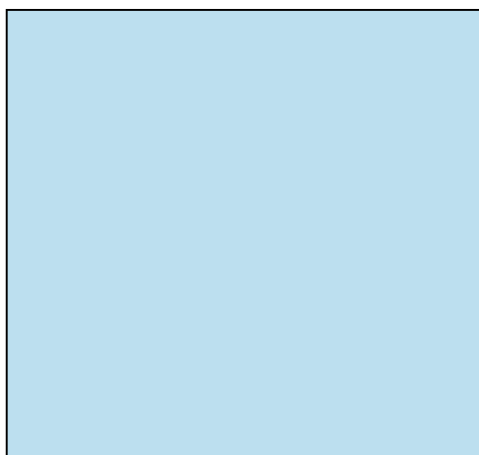
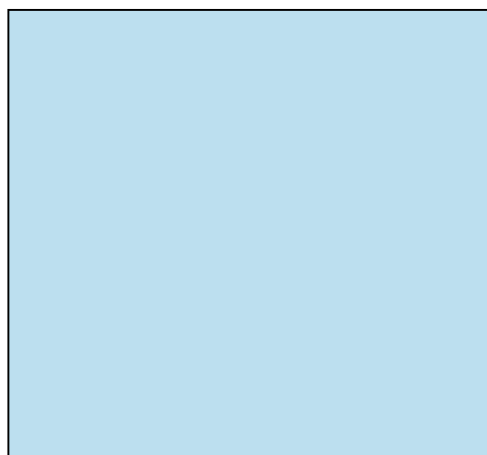
“Who We Tested”

- **Each run had different participants, but the data include runs from...**
- **Abaca, Barracuda, Brightmail, Ciphertrust, Cloudmark, Commtouch, Exchange 2007, Frontbridge, GFI, Heluna, Ironport, MailShell, Postini, Proofpoint, SonicWALL, Sophos, SpamStopsHere, StarEngine, Threatwall, Trend Micro, Tumbleweed, Untangle, Watchguard and 2 others that don't have names**

Securing Email, Messaging Platforms and Mobile Devices

Myth 1: All Products Are The Same

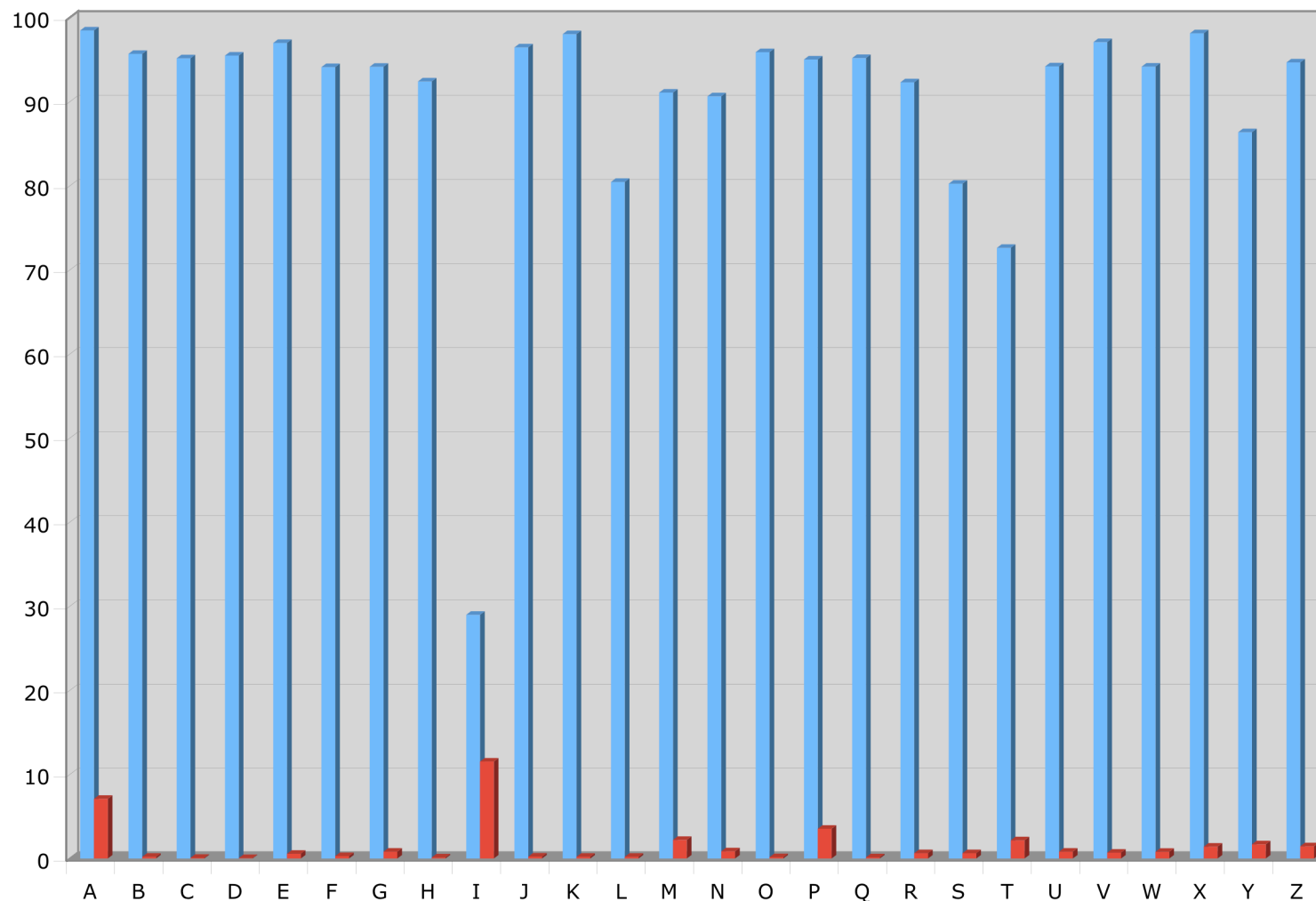
- **More specifically: “All Spam Engines are the same. You should buy based on features.”**
- **Why? Lots of reasons...**



Securing Email, Messaging Platforms and Mobile Devices

Reality: Different Spam Engines Perform Differently

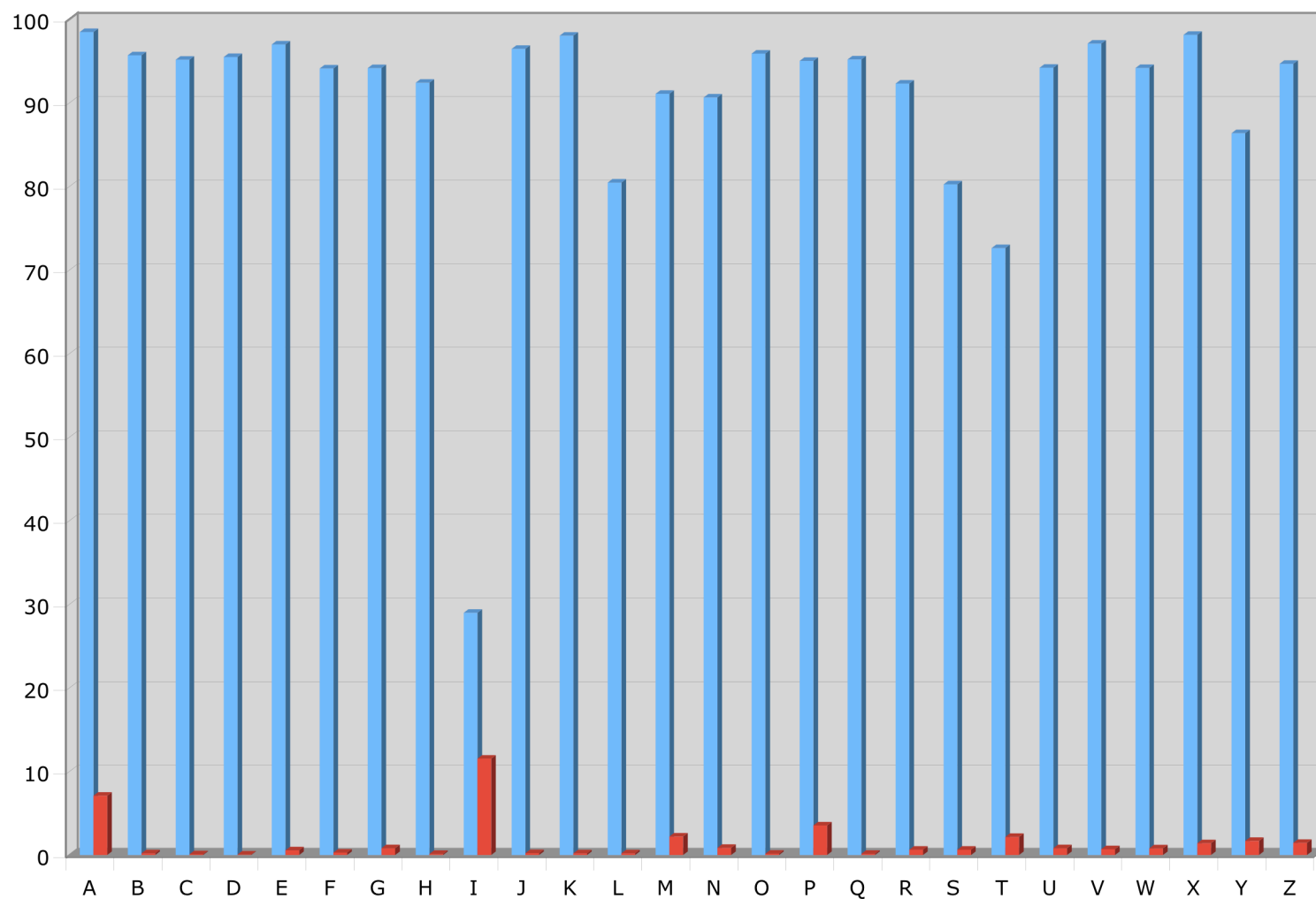
Most recent results for 26 different products



Securing Email, Messaging Platforms and Mobile Devices

Reality: Different Spam Engines Perform Differently

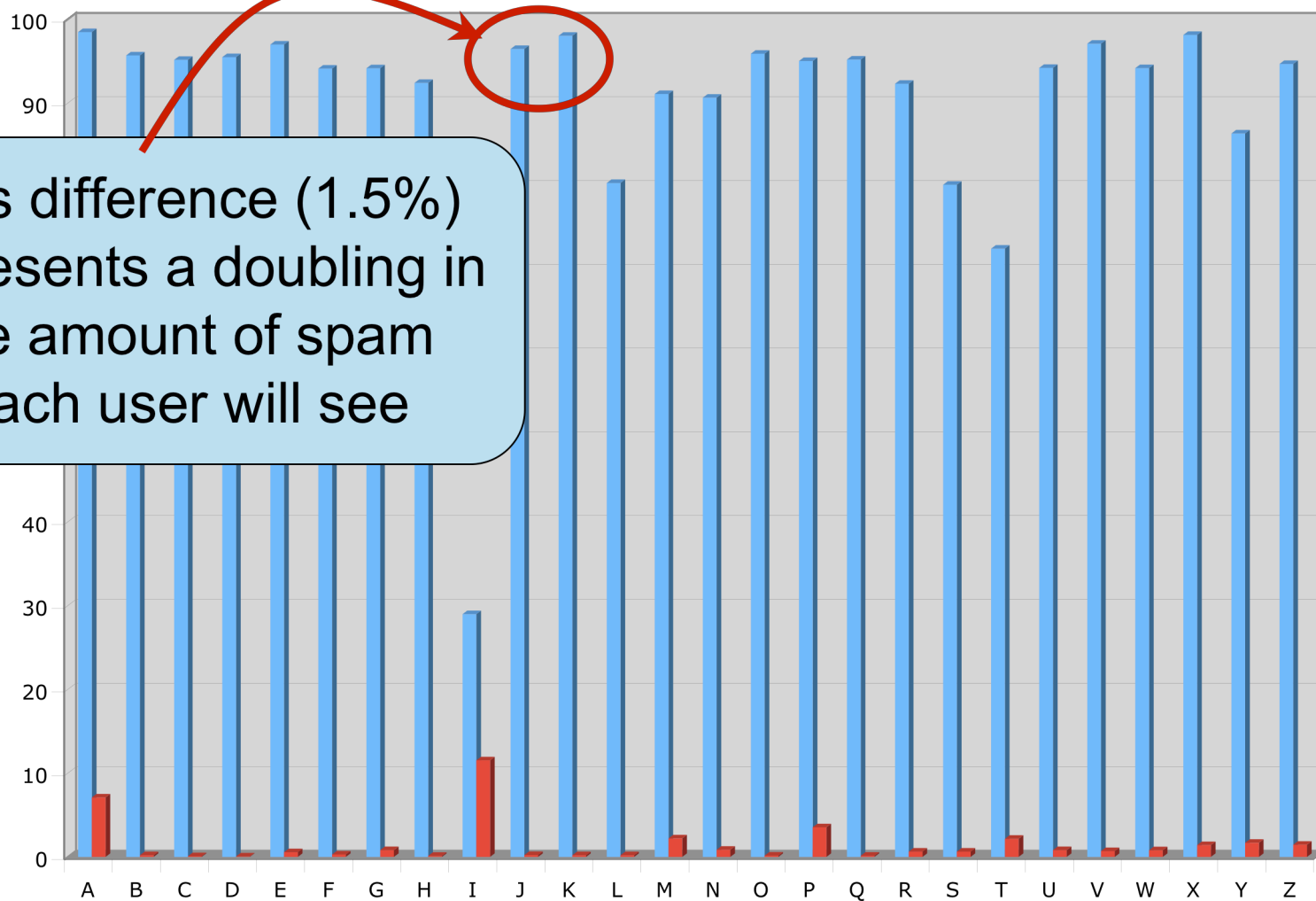
Most recent results for 26 different products



Securing Email, Messaging Platforms and Mobile Devices

Reality: Different Spam Engines Perform Differently

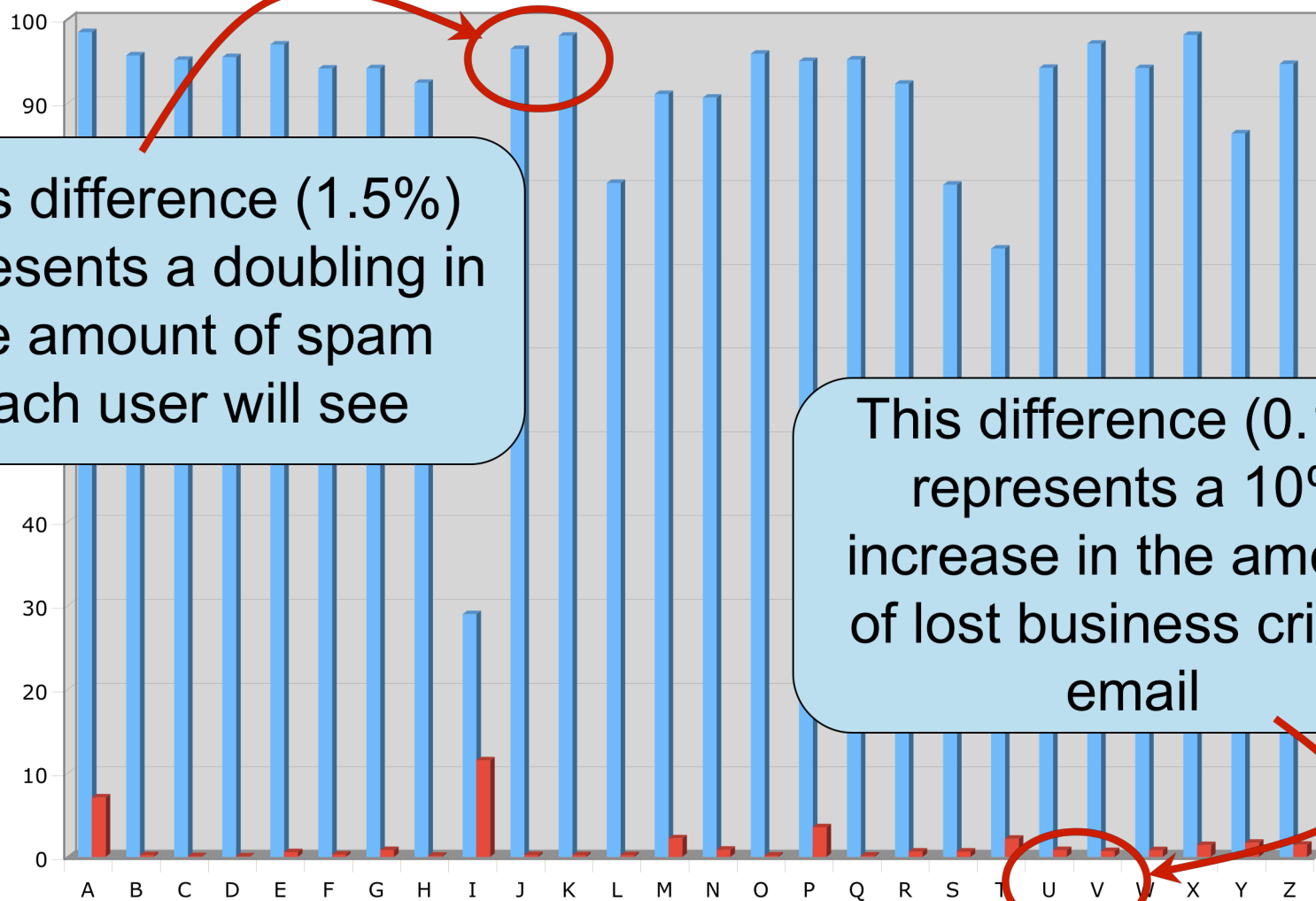
Most recent results for 26 different products



Securing Email, Messaging Platforms and Mobile Devices

Reality: Different Spam Engines Perform Differently

Most recent results for 26 different products



This difference (1.5%) represents a doubling in the amount of spam each user will see

This difference (0.1%) represents a 10% increase in the amount of lost business critical email

Securing Email, Messaging Platforms and Mobile Devices

Myth 2:

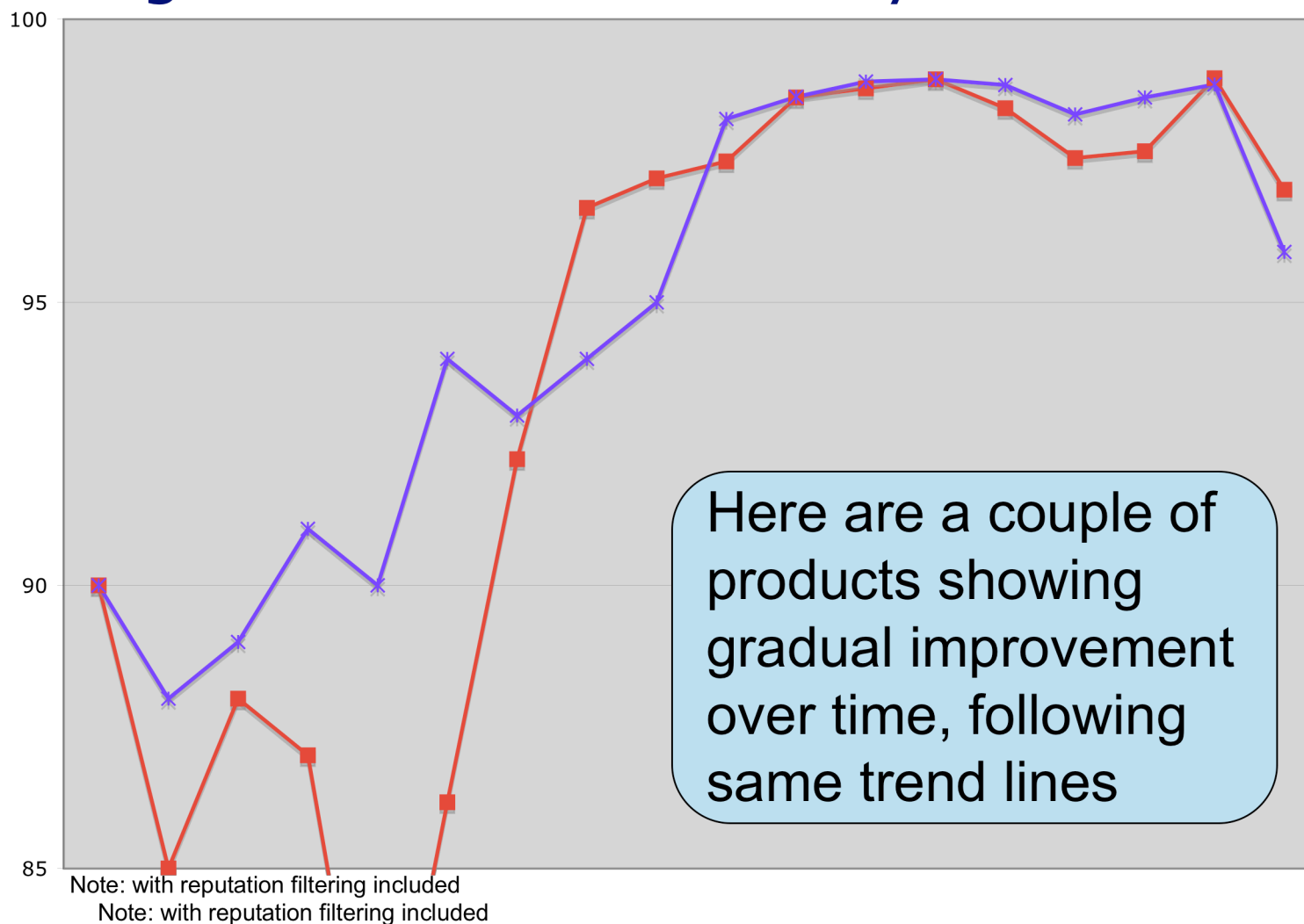
Great Products Stay Great

- **... And Bad Products Stay Bad**

Securing Email, Messaging Platforms and Mobile Devices

Reality:

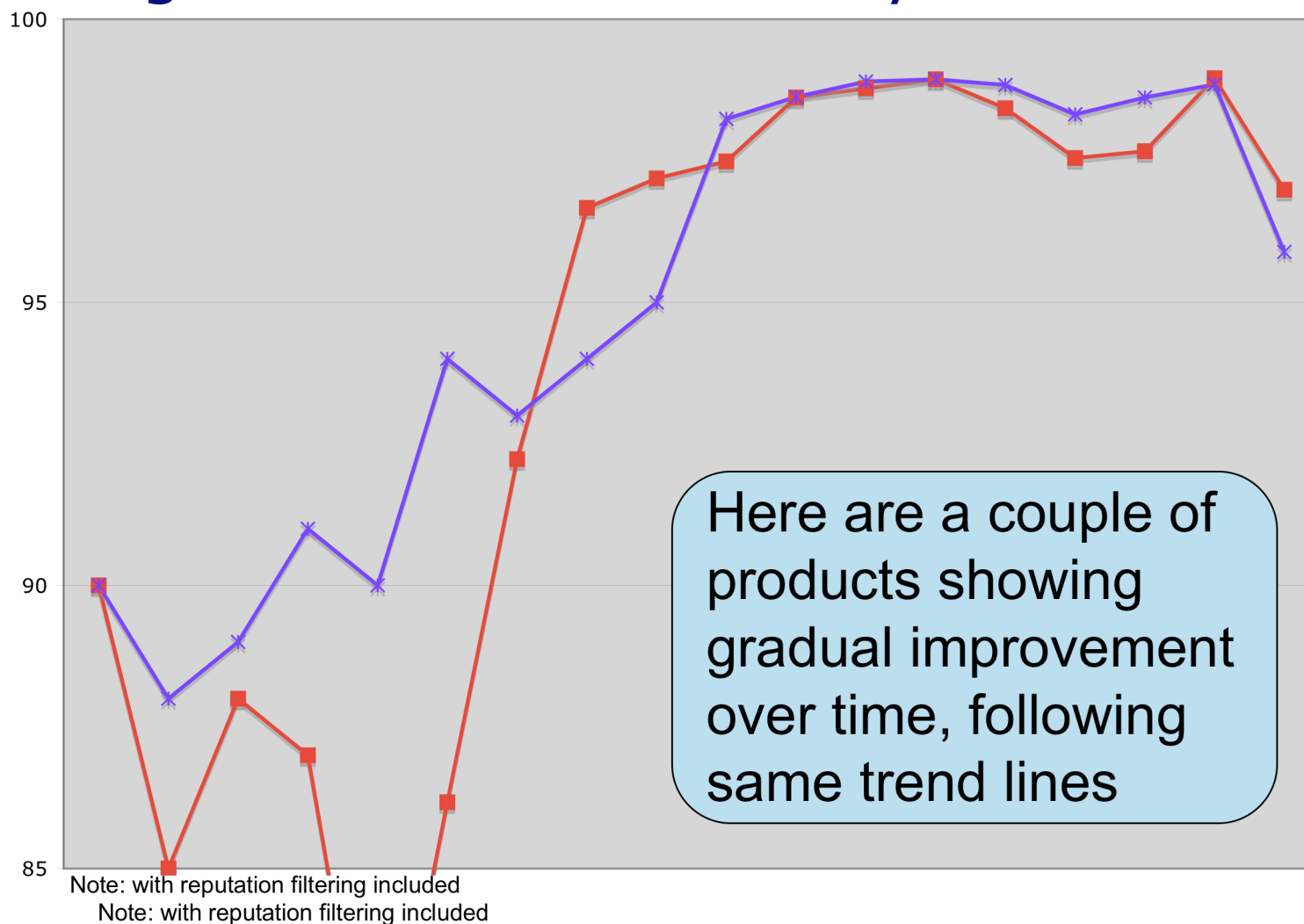
Each Engine Has Its Own Lifecycle



Securing Email, Messaging Platforms and Mobile Devices

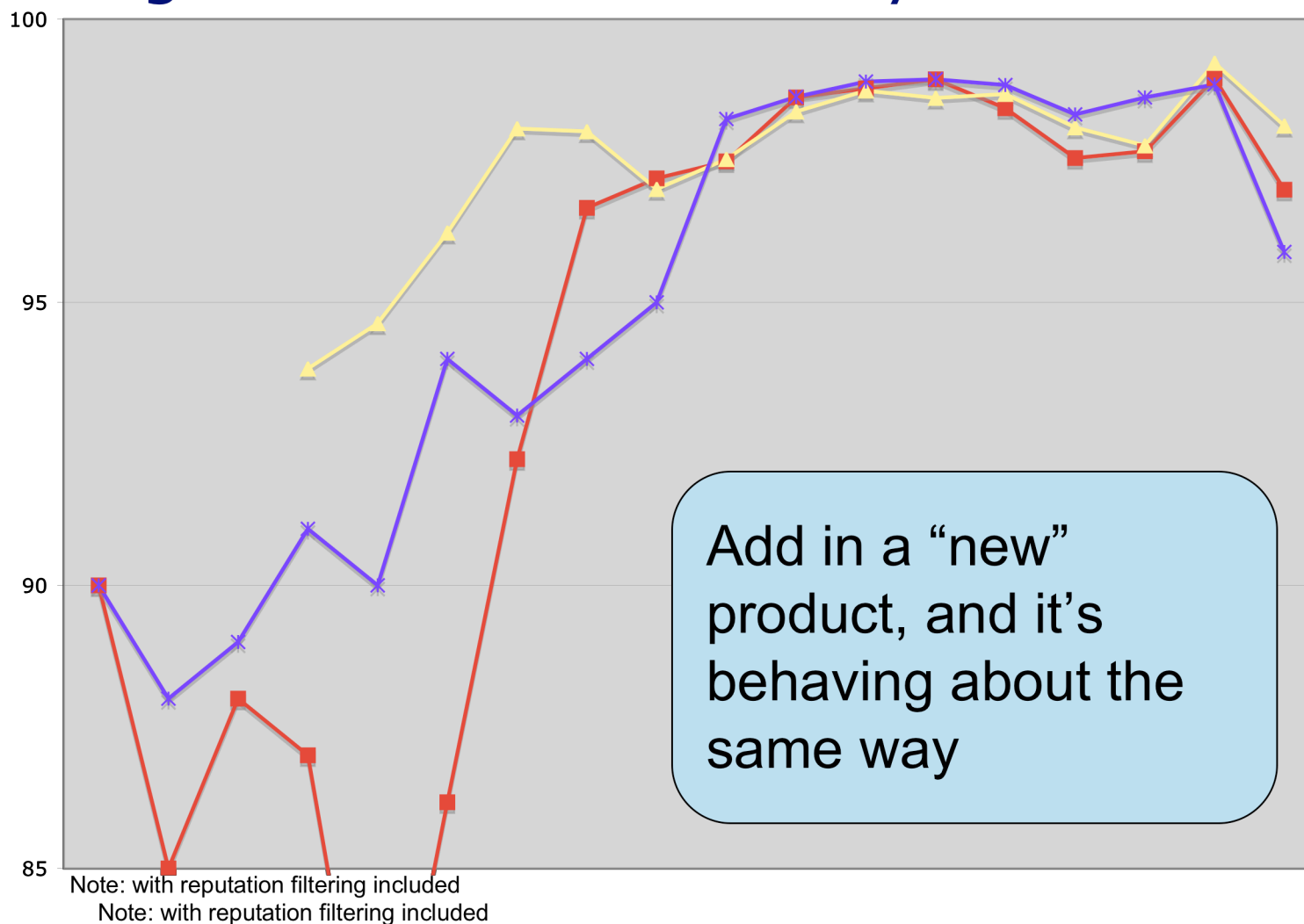
Reality:

Each Engine Has Its Own Lifecycle



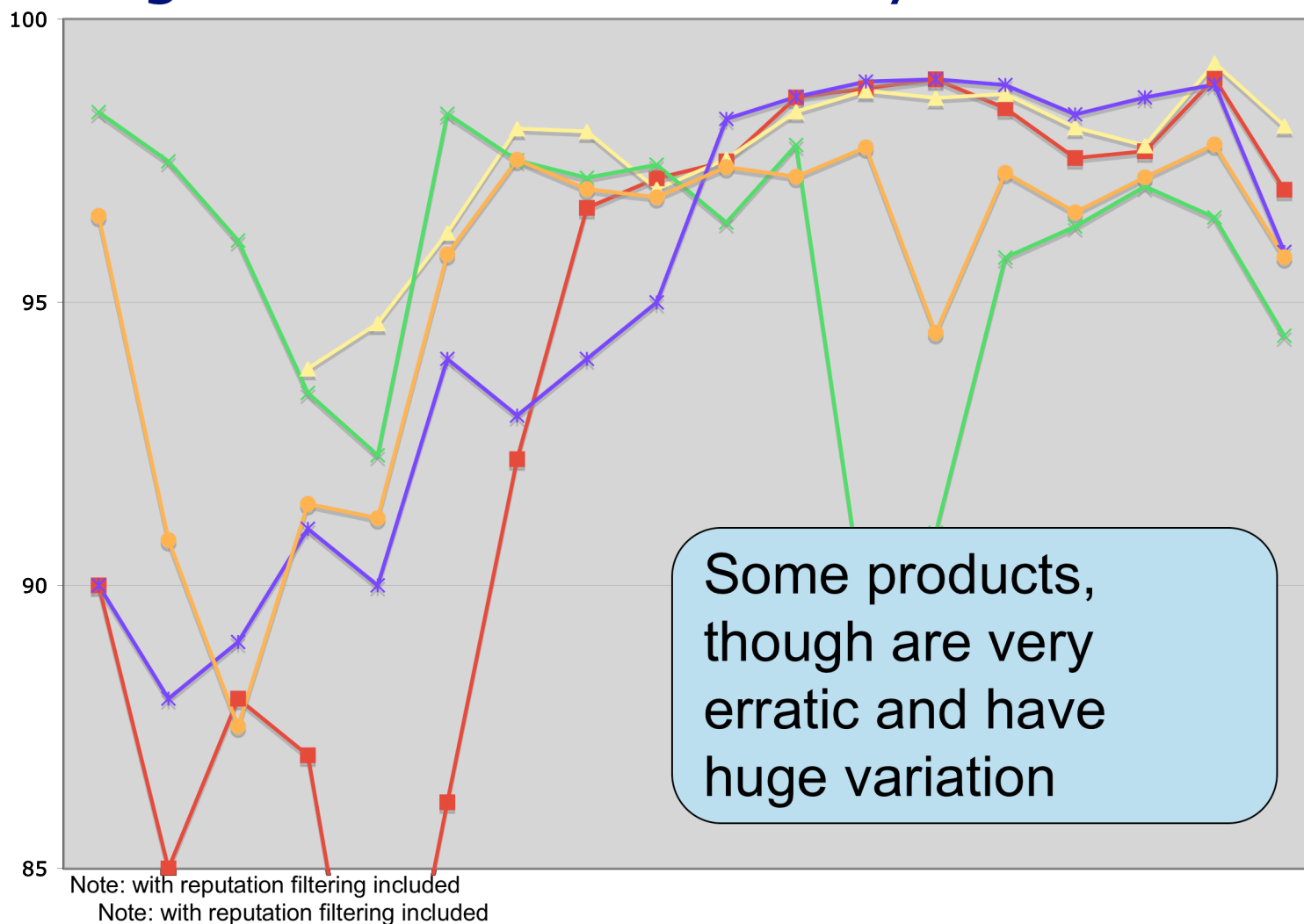
Securing Email, Messaging Platforms and Mobile Devices

Reality: Each Engine Has Its Own Lifecycle



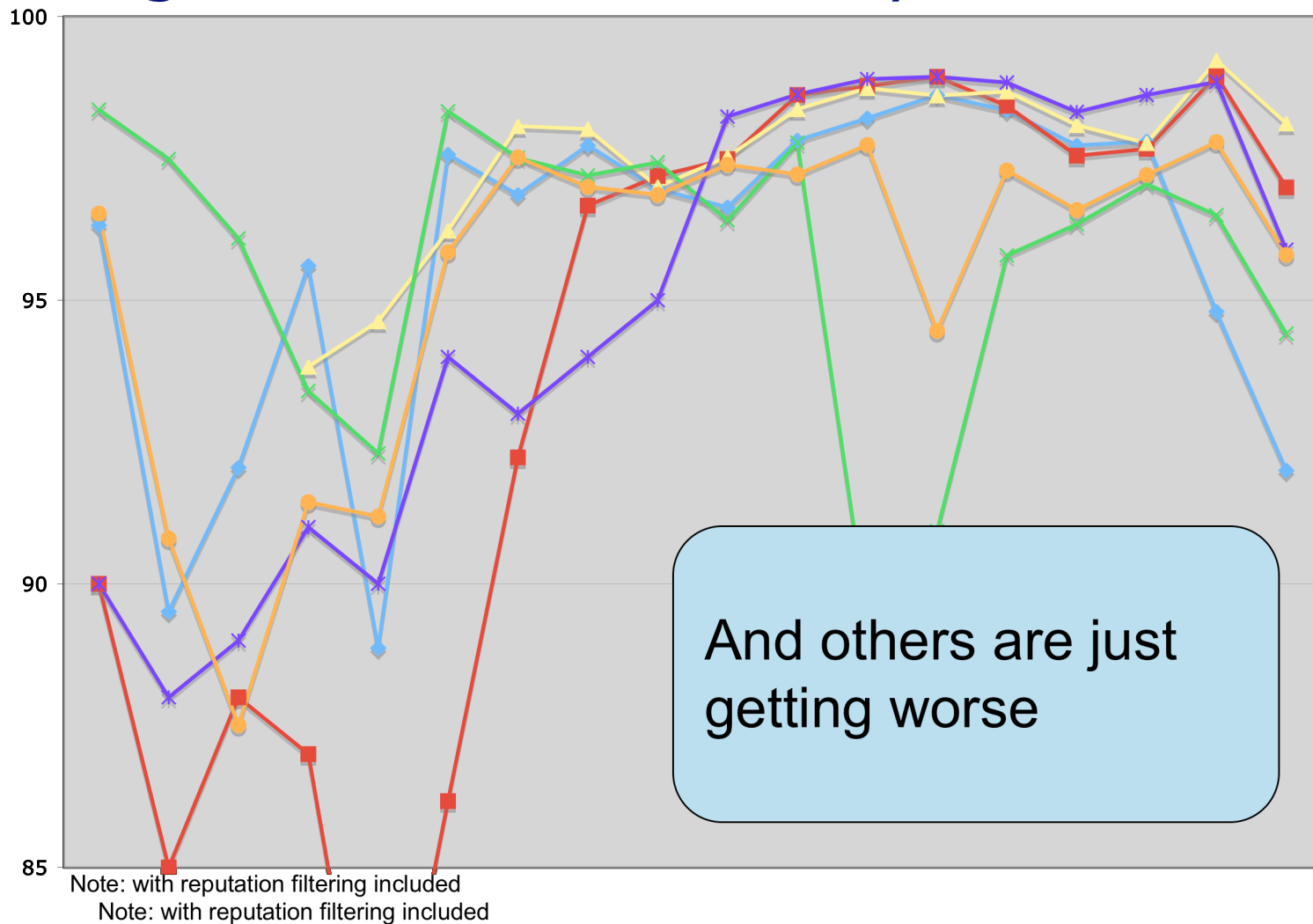
Securing Email, Messaging Platforms and Mobile Devices

Reality: Each Engine Has Its Own Lifecycle



Securing Email, Messaging Platforms and Mobile Devices

Reality: Each Engine Has Its Own Lifecycle



Securing Email, Messaging Platforms and Mobile Devices

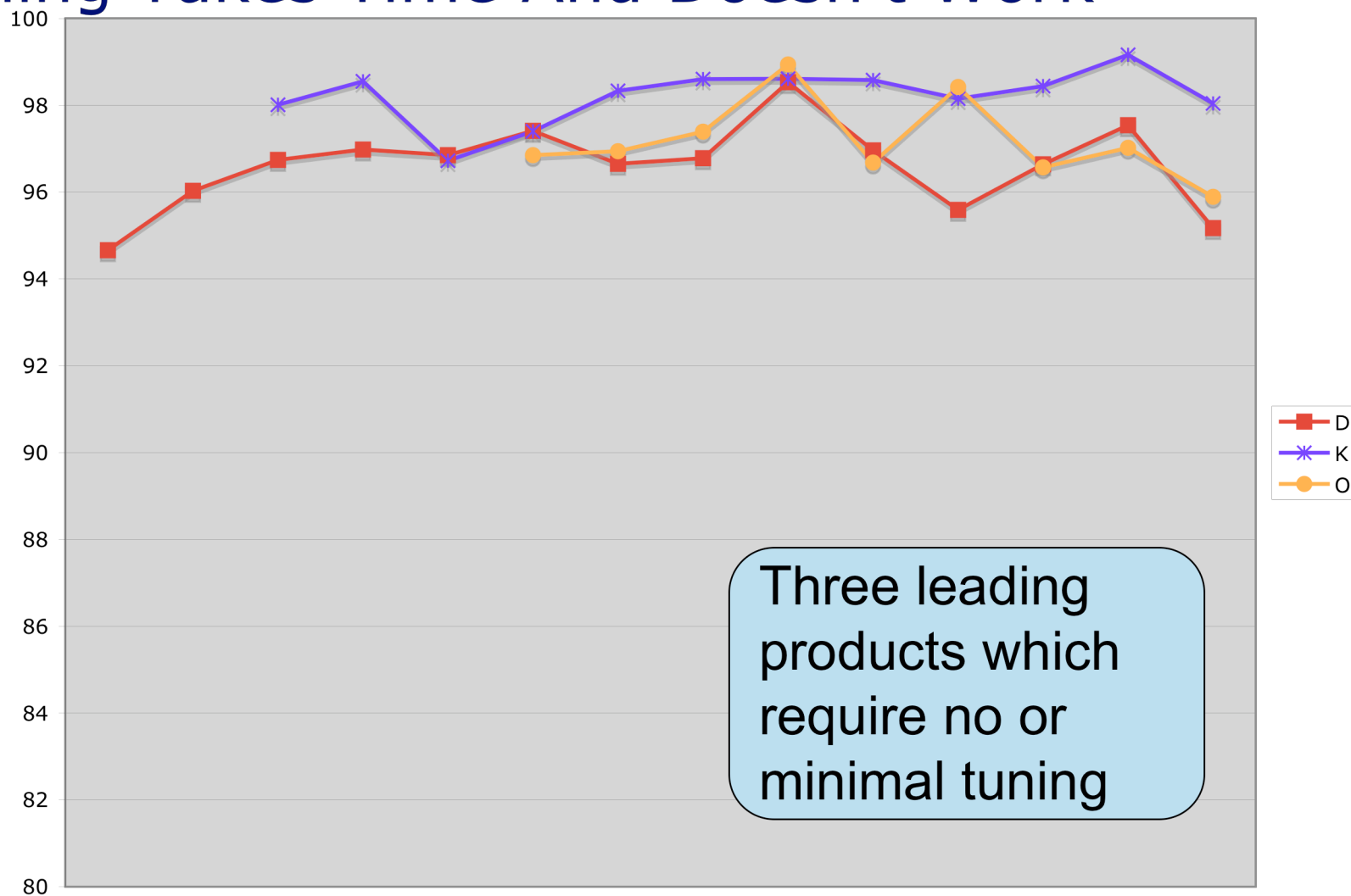
Myth 3: Training And Tuning Products Is Good

- **Where does this one come from?**
 - **Technology Guru installs Spam Assassin**
 - **Spam Assassin requires training**
 - **Technology Guru is happy**
 - **Ergo: Spam Filtering requires Training**
 - **Q.E.D.**

Tuning is a spectrum... all products allow for some tuning. We're just differentiating between levels of adjustment.

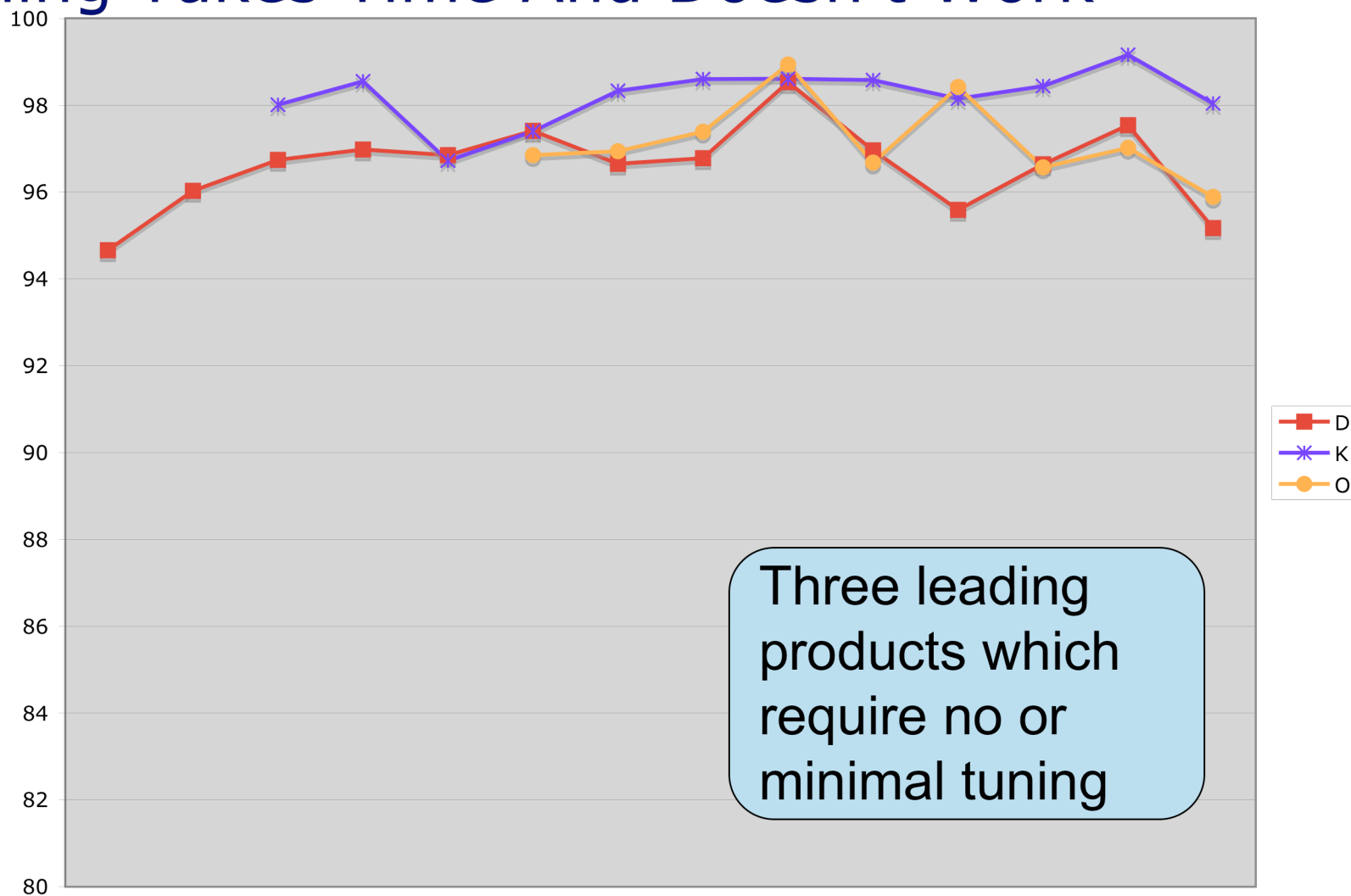
Securing Email, Messaging Platforms and Mobile Devices

Reality: Training Takes Time And Doesn't Work



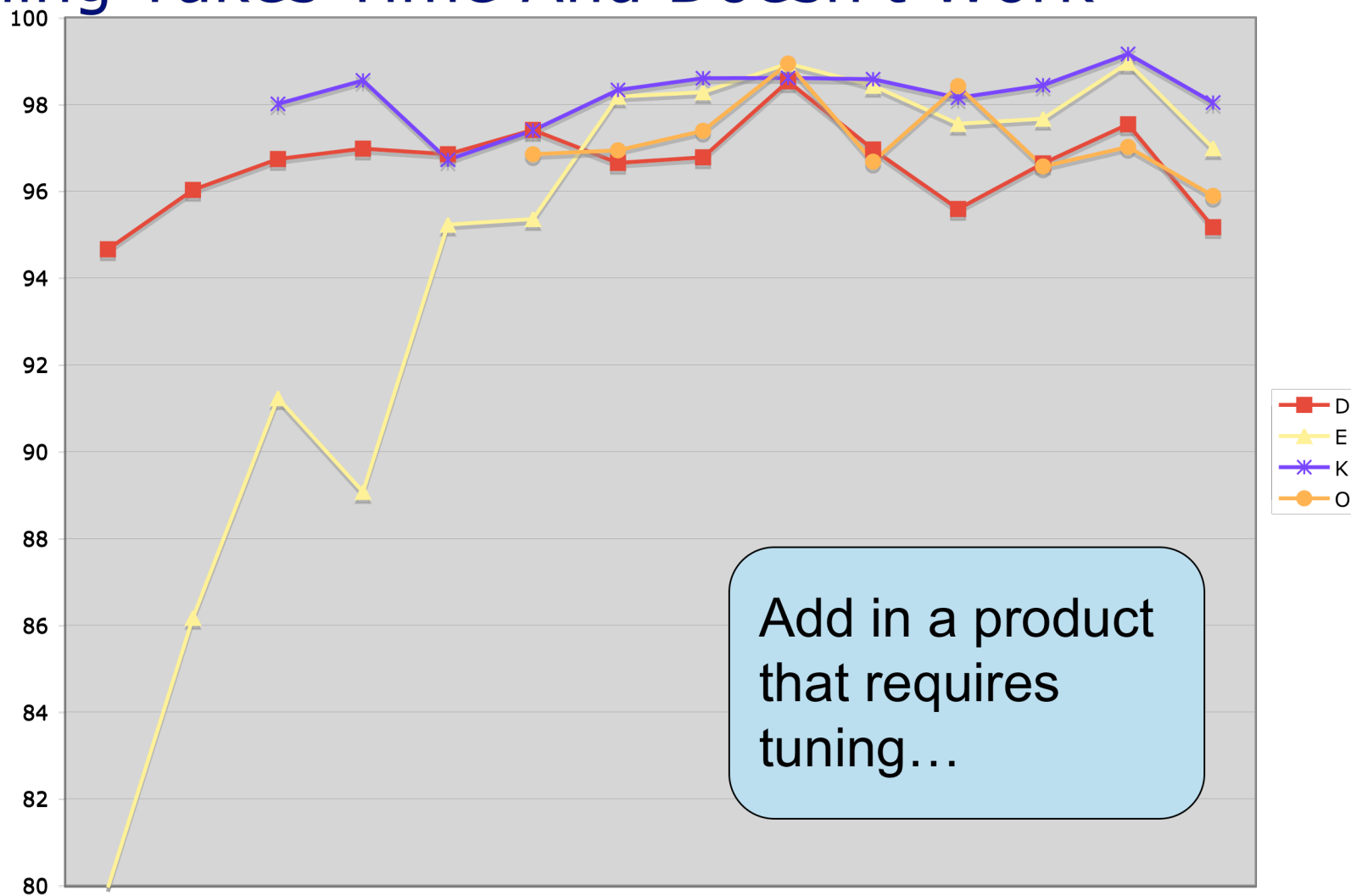
Securing Email, Messaging Platforms and Mobile Devices

Reality: Training Takes Time And Doesn't Work



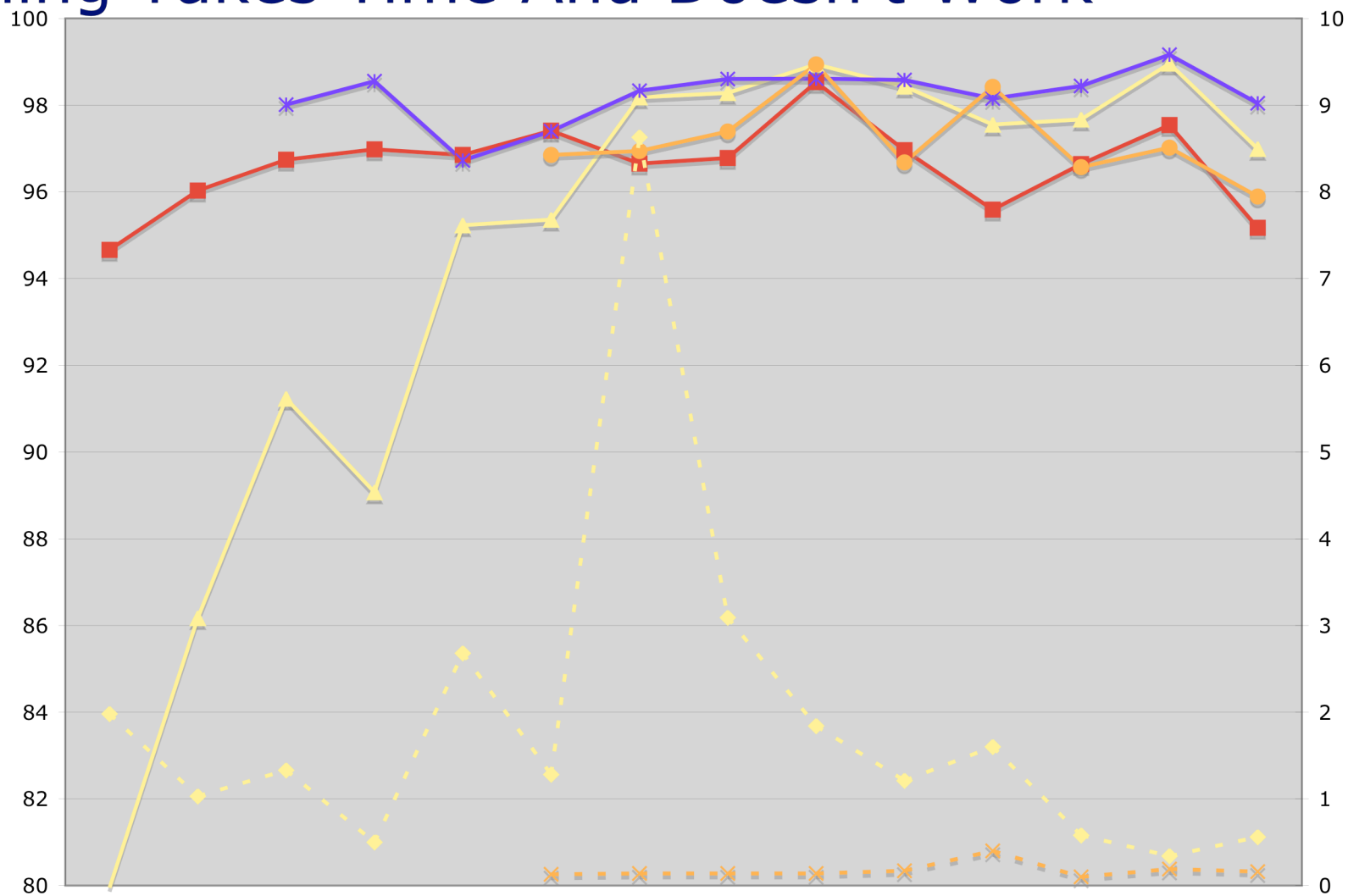
Securing Email, Messaging Platforms and Mobile Devices

Reality: Training Takes Time And Doesn't Work



Securing Email, Messaging Platforms and Mobile Devices

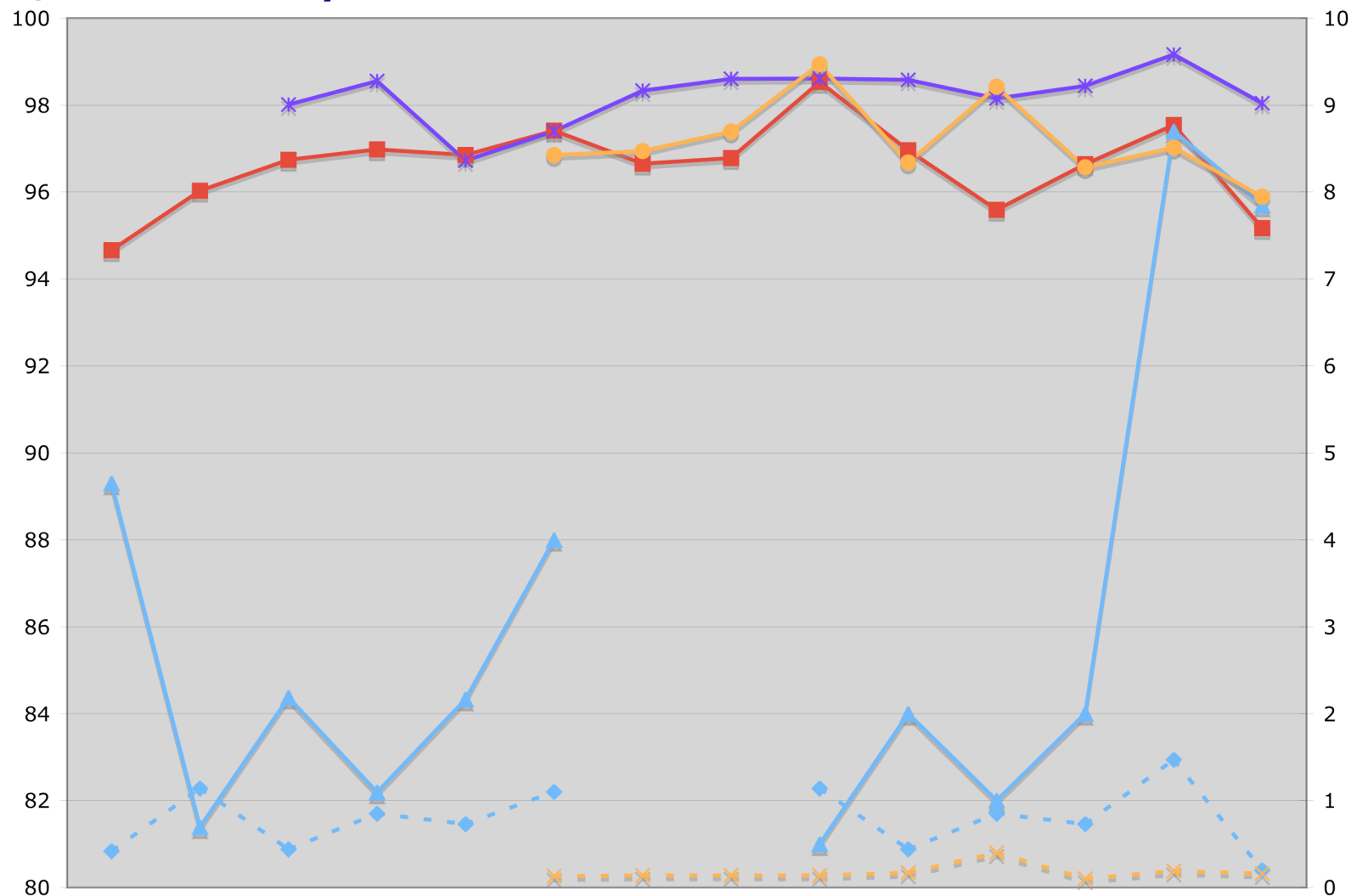
Reality: Training Takes Time And Doesn't Work



Securing Email, Messaging Platforms and Mobile Devices

More Reality:

OK, Let's Try A Different Product



Securing Email, Messaging Platforms and Mobile Devices

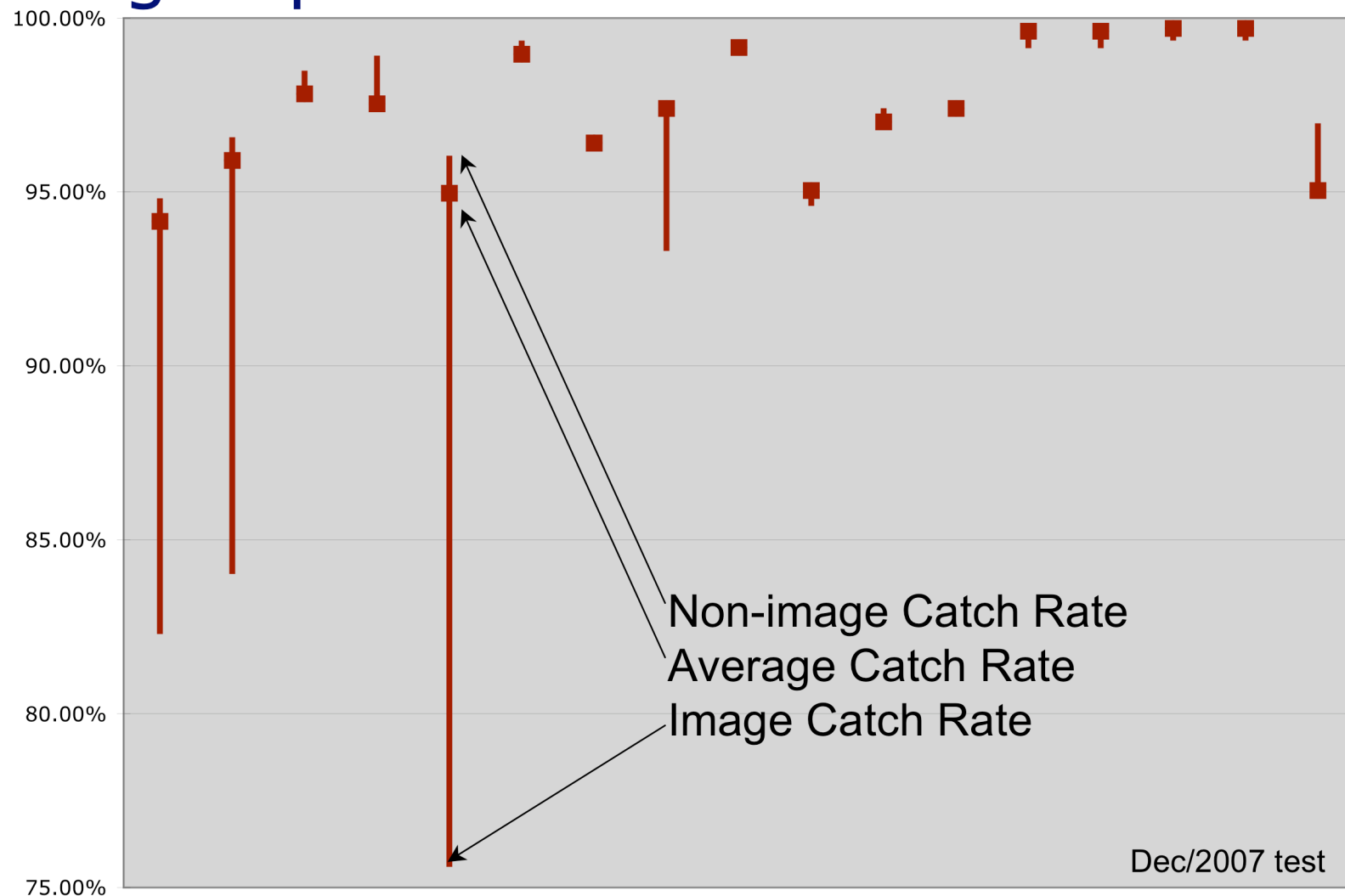
Myth 4: Image Spam Is A Problem

- **Where does this one come from?**
 - **Image spam is invented**
 - **Some products can't handle it**
 - **Strategy? Send out a press release explaining how awful life is, and maybe your customers will let you live while you fix it**

Securing Email, Messaging Platforms and Mobile Devices

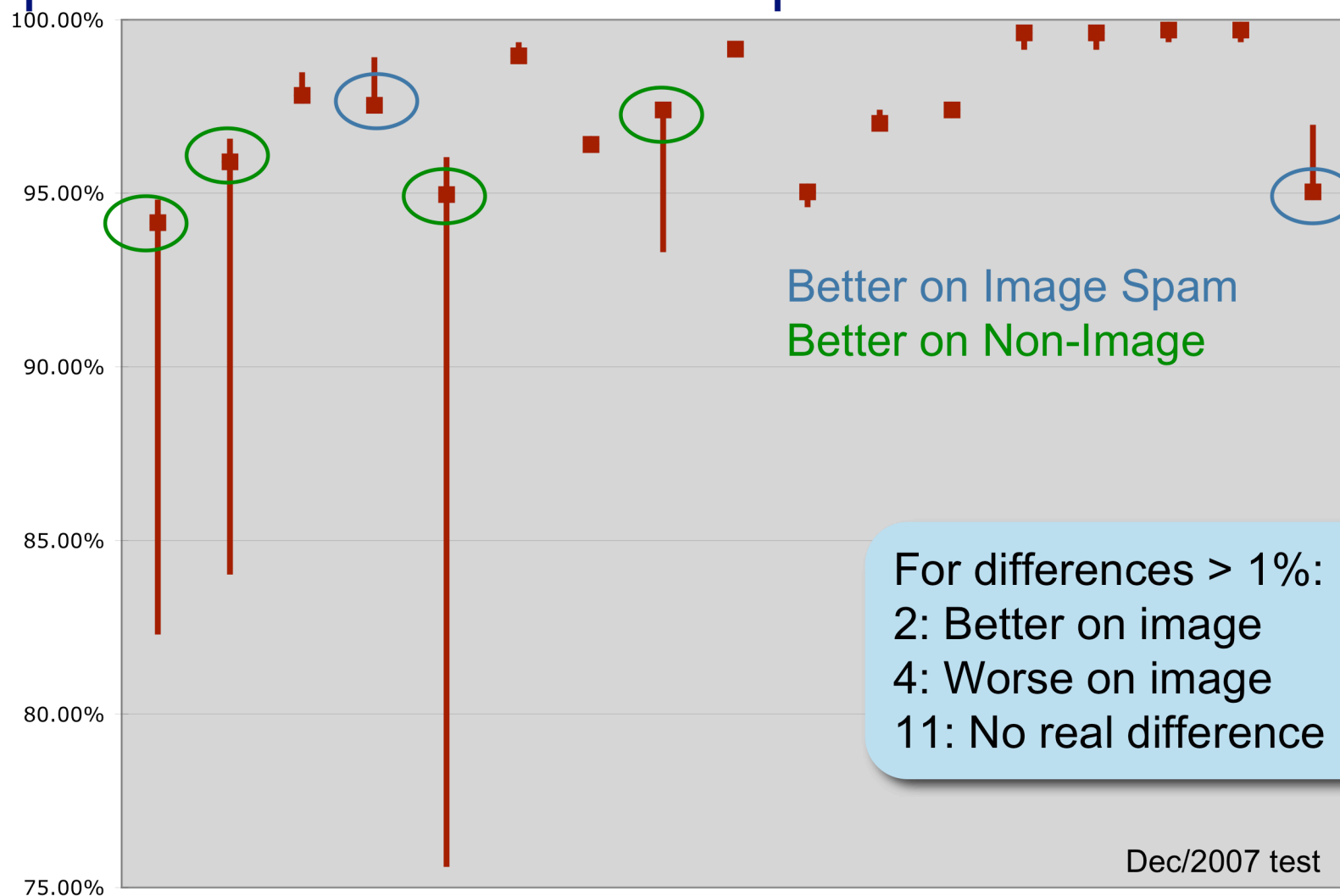
Reality:

Image Spam Is Not A Problem - For Most



Securing Email, Messaging Platforms and Mobile Devices

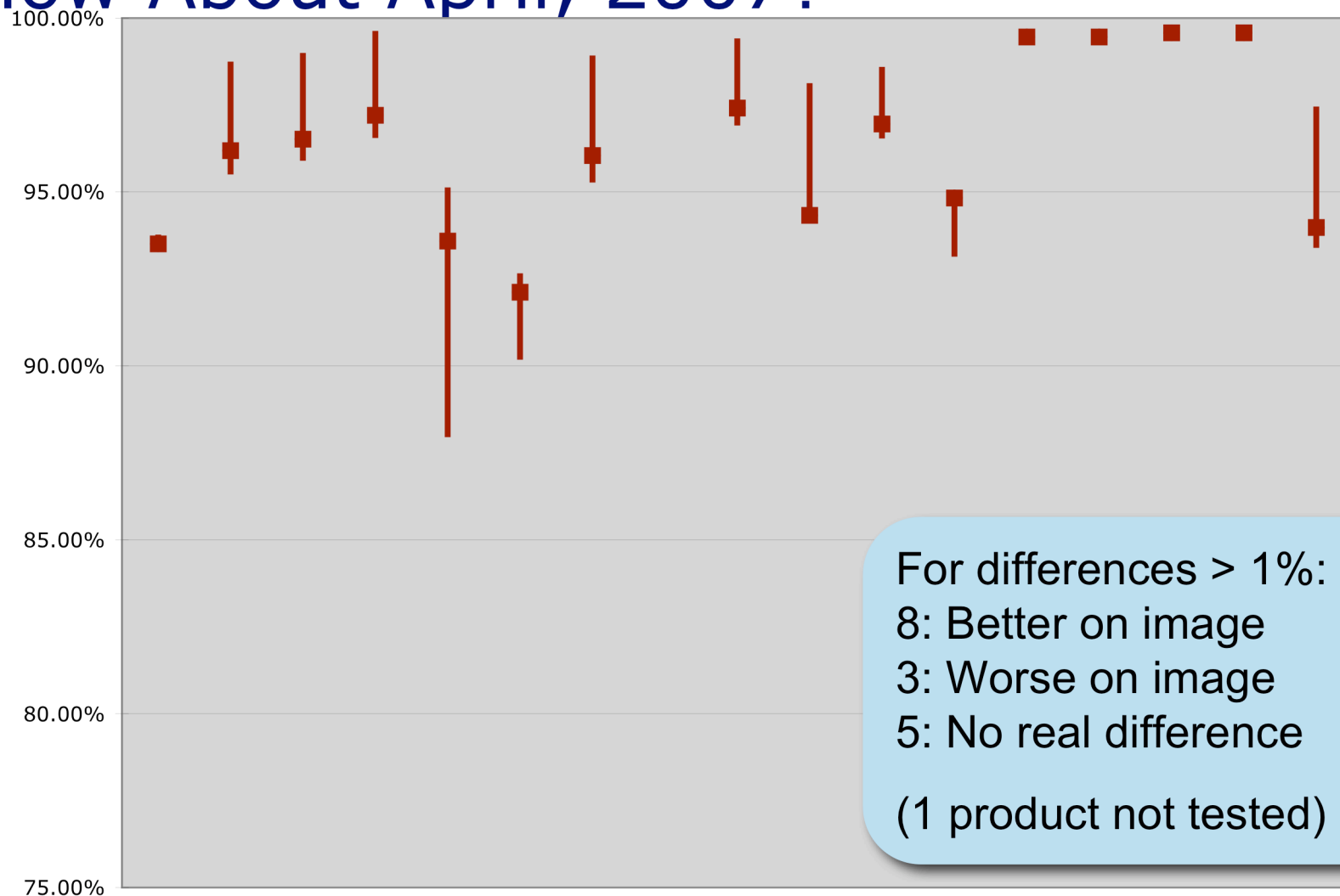
In Fact, Some Products Do Better On Image Spam Than On Normal Spam



Securing Email, Messaging Platforms and Mobile Devices

OK, You Got Me...

How About April, 2007?



Securing Email, Messaging Platforms and Mobile Devices

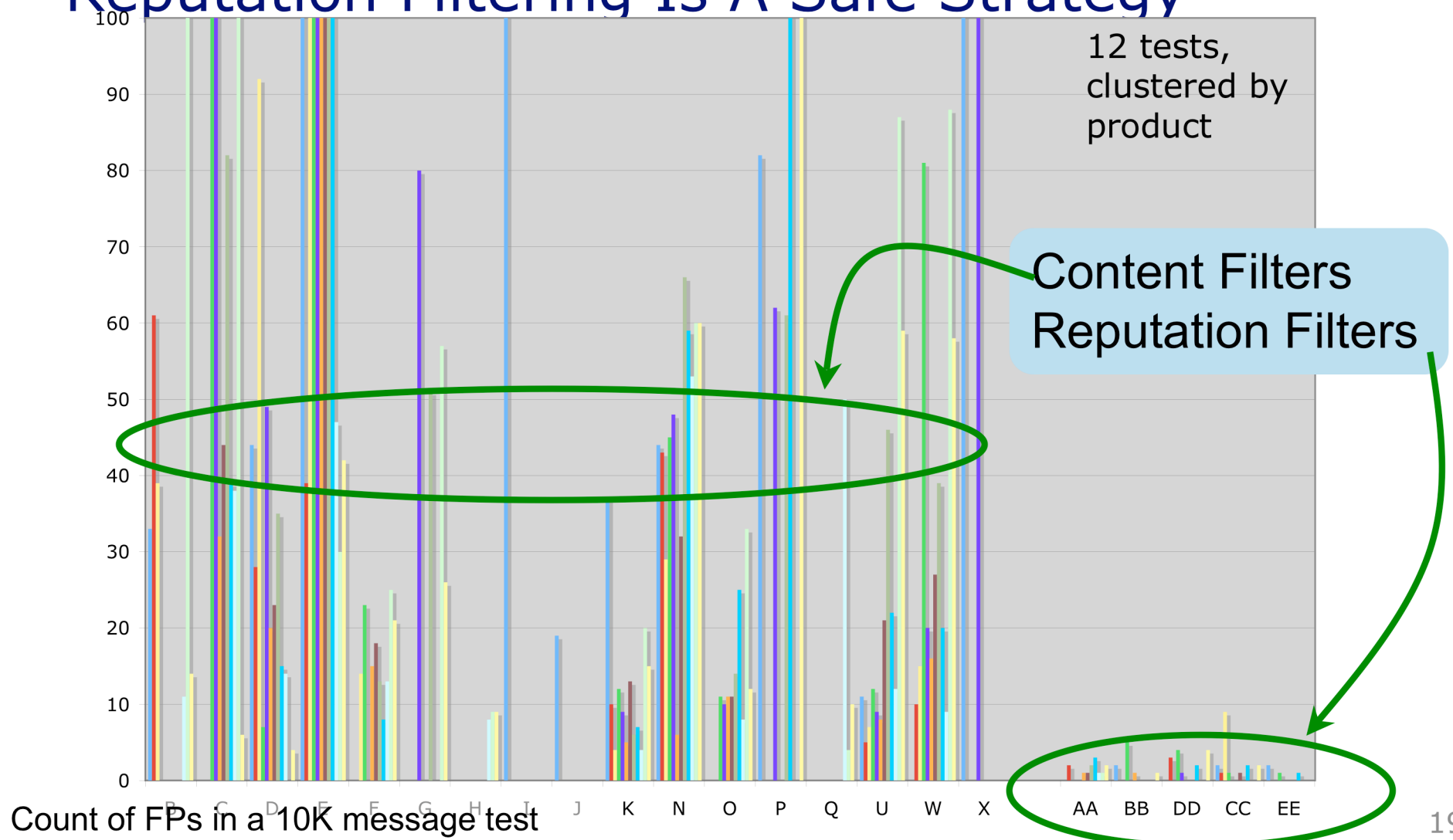
Myth 5: Reputation Filtering Is Dangerous

- ... and leads to false positives

Securing Email, Messaging Platforms and Mobile Devices

Reality:

Reputation Filtering Is A Safe Strategy



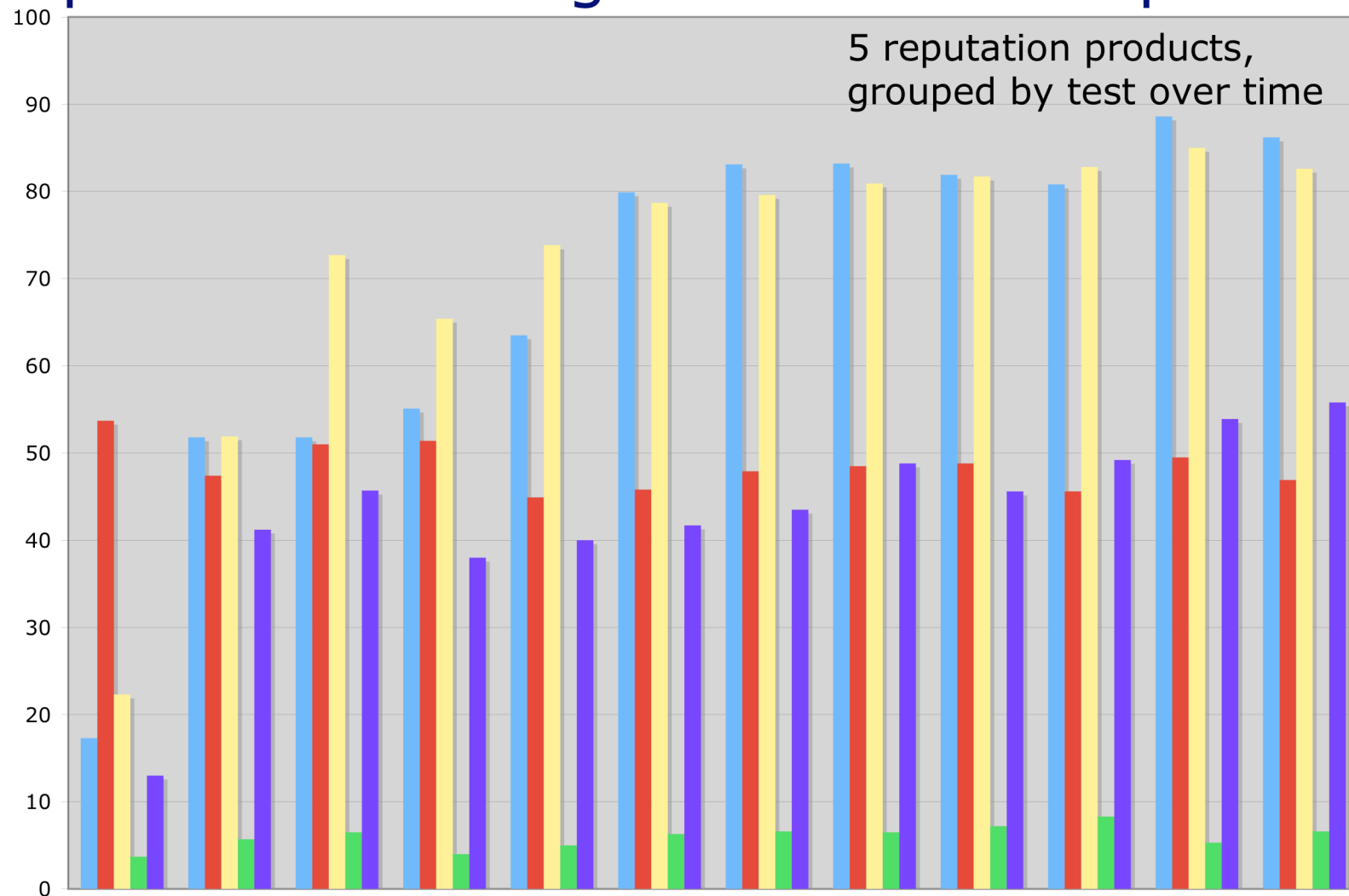
Securing Email, Messaging Platforms and Mobile Devices

Myth 6: You Should Accept The Mail, And Then Apply Reputation Filtering

- **Where does this one come from?**
 - **Some products can't do reputation filtering because they don't have their own SMTP receiver**
 - **These products grovel through headers and simulate reputation filtering**
 - **Other products use reputation as one factor in deciding to mark mail as "Spam"**

Securing Email, Messaging Platforms and Mobile Devices

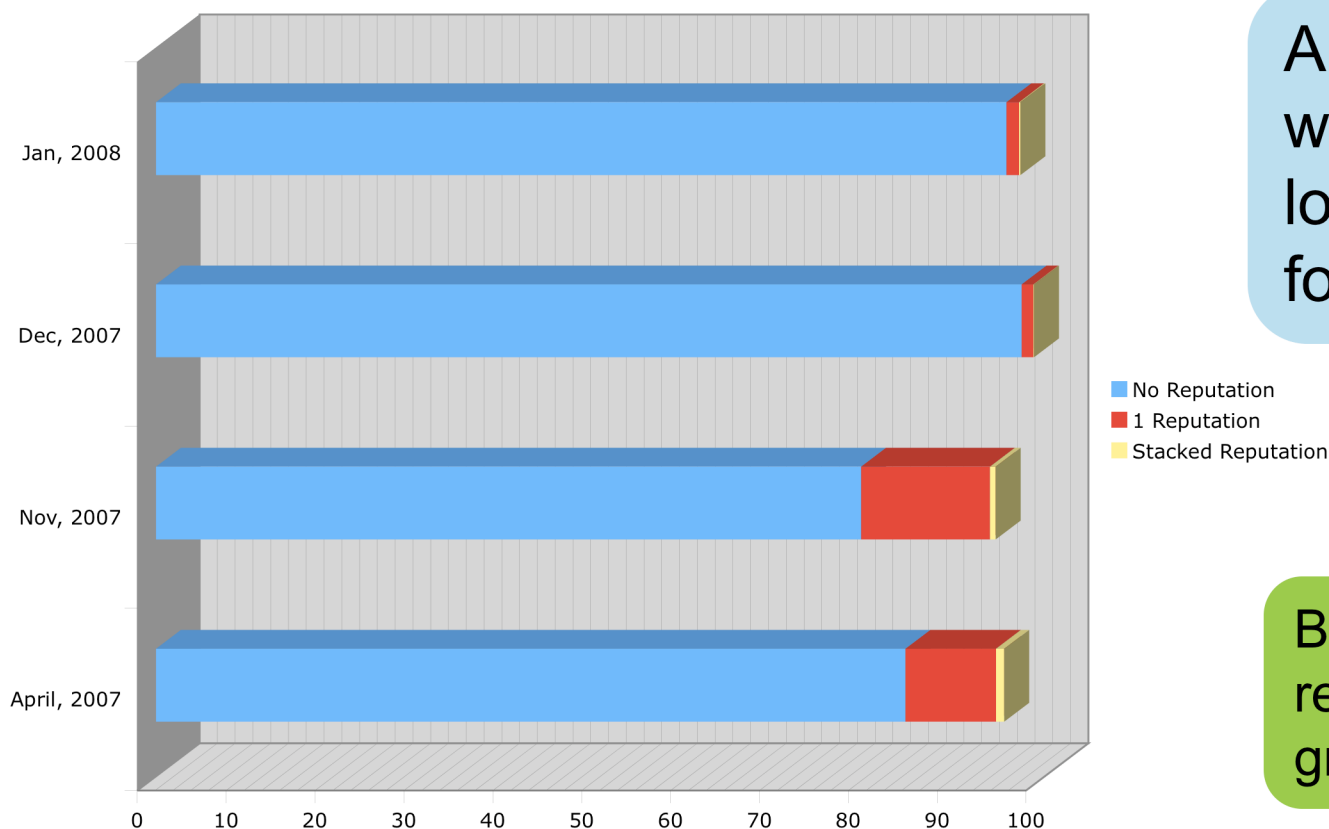
Reality: Reputation Filtering Blocks Lots of Spam



Securing Email, Messaging Platforms and Mobile Devices

Interesting Side Question: Should I Stack Reputation Services?

- **After all, if one is good, aren't two better?**



Answer: Not really worth it for traffic load and potential for false positives

But this doesn't really reflect the value of graylisting...

Securing Email, Messaging Platforms and Mobile Devices

Myth 7:

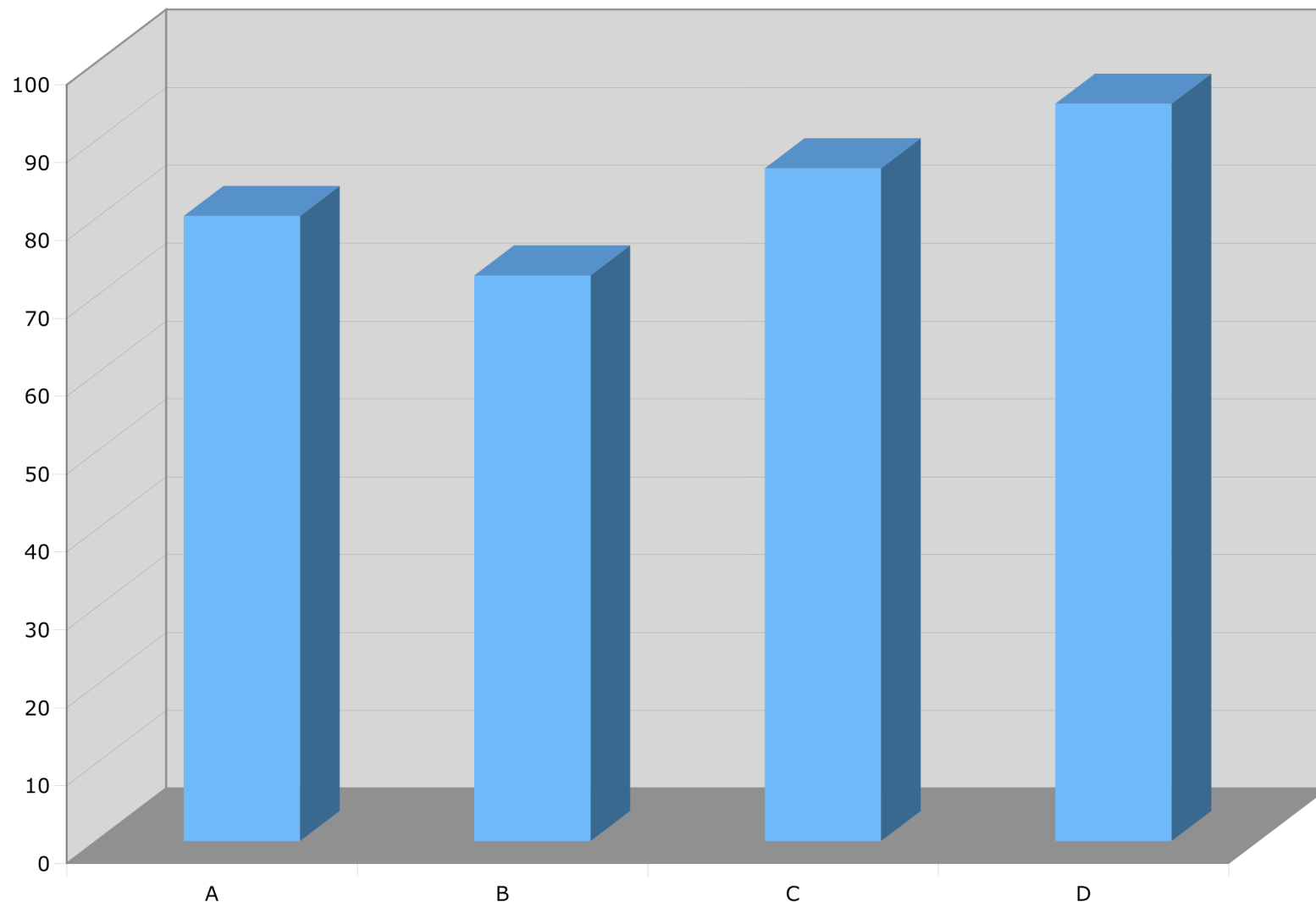
UTM Is A Good Way To Do Anti-Spam

- **UTM promises to make life simple by centralizing and consolidating everything into a single place**
- **Several UTM products have anti-spam built into them**
- **So this must work, right?**

Securing Email, Messaging Platforms and Mobile Devices

Reality:

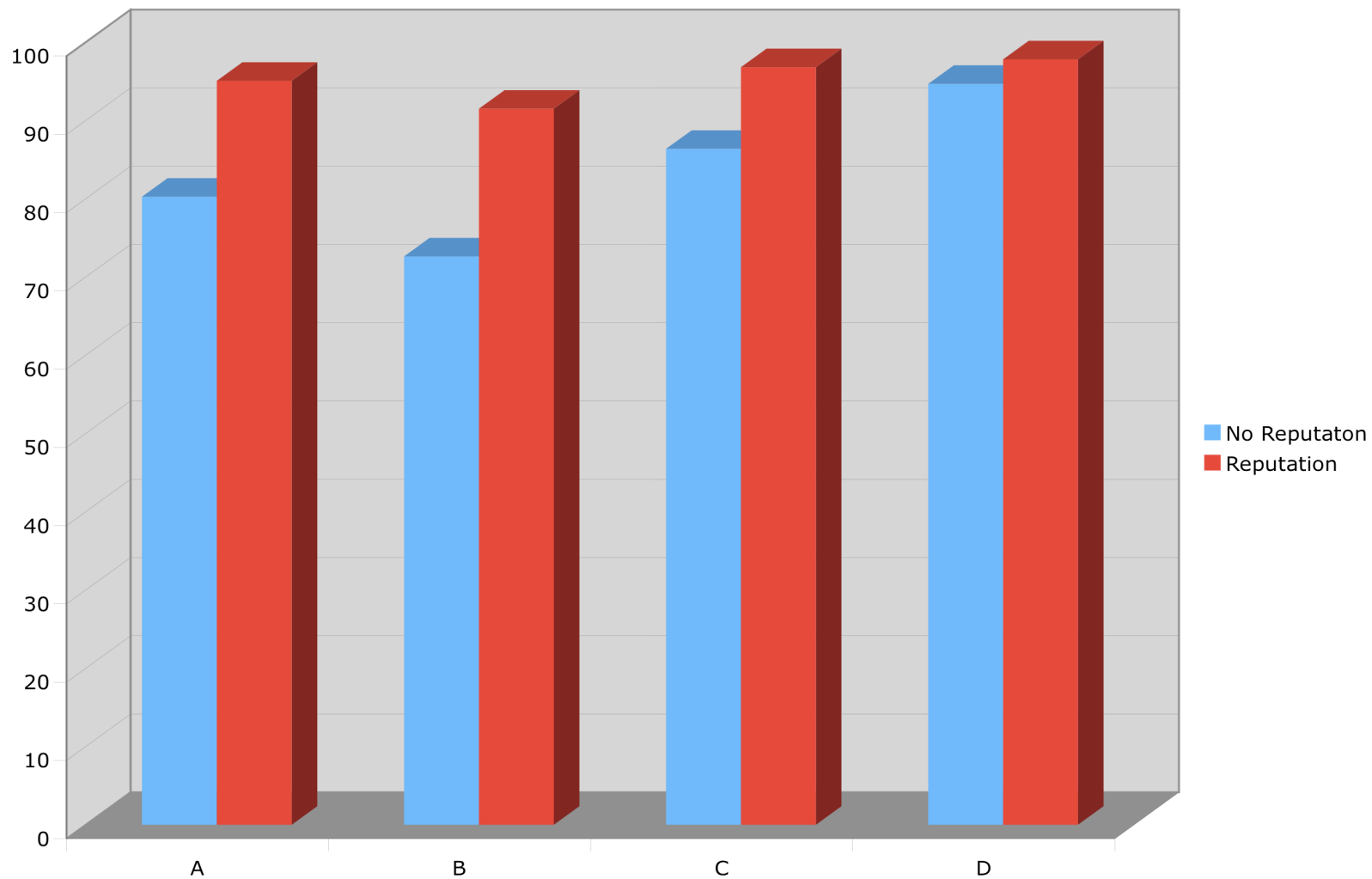
UTM Anti-Spam As Tested Doesn't Work



Securing Email, Messaging Platforms and Mobile Devices

Reality:

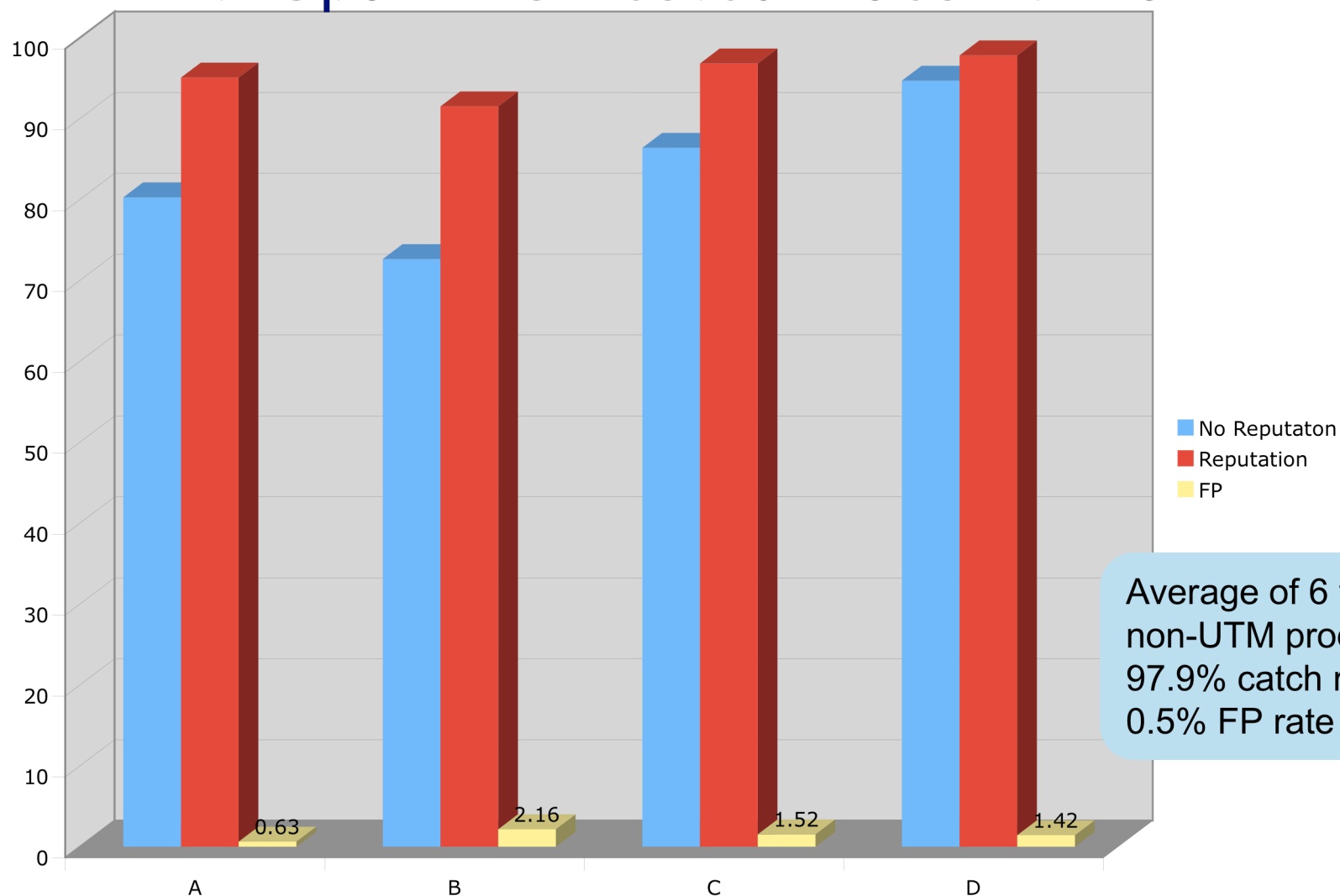
UTM Anti-Spam As Tested Doesn't Work



Securing Email, Messaging Platforms and Mobile Devices

Reality:

UTM Anti-Spam As Tested Doesn't Work



Securing Email, Messaging Platforms and Mobile Devices

Thanks!

Joel Snyder
Senior Partner
Opus One
jms@opus1.com

