

YAHOO!

AppSec is Eating Security

PRESENTED BY **Alex Stamos** | AppSec Cali | January 27, 2015

Why Software Is Eating The World

By MARC ANDREESSEN

August 20, 2011

This week, Hewlett-Packard (where I am on the board) announced that it is exploring jettisoning its struggling PC business in favor of investing more heavily in software, where it sees better potential for growth. Meanwhile, Google plans to buy up the cellphone handset maker Motorola Mobility. Both moves surprised the tech world. But both moves are also in line with a trend I've observed, one that makes me optimistic about the future growth of the American and world economies, despite the recent turmoil in the stock market.



In short, software is eating the world.

More than 10 years after the peak of the 1990s dot-com bubble, a dozen or so new Internet companies like Facebook and Twitter are sparking controversy in Silicon Valley, due to their rapidly growing private market

Most enterprises are not safe



Most enterprises are not safe

“SECURE 100”

FORTUNE
500

- Big Banks + other FIs
- Defense Industrial Base
- Oil and Gas
- Critical Infrastructure
- Big Tech
- Some Retail

Most enterprises are not safe



"SECURE 100"

- Big Banks + other FIs
- Defense Industrial Base
- Oil and Gas
- Critical Infrastructure
- Big Tech
- Some Retail

"TOASTED 400"

Everybody Else

Most enterprises are not safe



"SECURE 100"

- Big Banks + other FIs
- Defense Industrial Base
- Oil and Gas
- Critical Infrastructure
- Big Tech
- Some Retail

"TOASTED 400"

Everybody Else

What are they missing?

- Secure software engineering
- Engineering focused IR
- Ability to create, not buy, solutions

Almost no users are safe

How My Mom Got Hacked

By ALINA SIMONE JAN. 2, 2015

Email

Share

Tweet

Save

More



MY mother received the ransomnote on the Tuesday before Thanksgiving. It popped up on her computer screen soon after she'd discovered that all of her files had been locked. "Your files are encrypted," it announced. "To get the key to decrypt files you have to pay 500 USD." If my mother failed to pay within a week, the price would go up to \$1,000. After that, her decryption key would be destroyed and any chance of accessing the 5,726 files on her PC — all of her data — would be lost forever.

Sincerely, CryptoWall.

CryptoWall 2.0 is the latest immuno-resistant strain of a larger body of viruses known as ransomware. The virus is thought to infiltrate your computer



Javier Jaén

Security hardware is becoming un-buyable



Arista 7508E
1152 x 10GbE
30Tbps backplane
5kW

Security hardware is becoming un-buyable

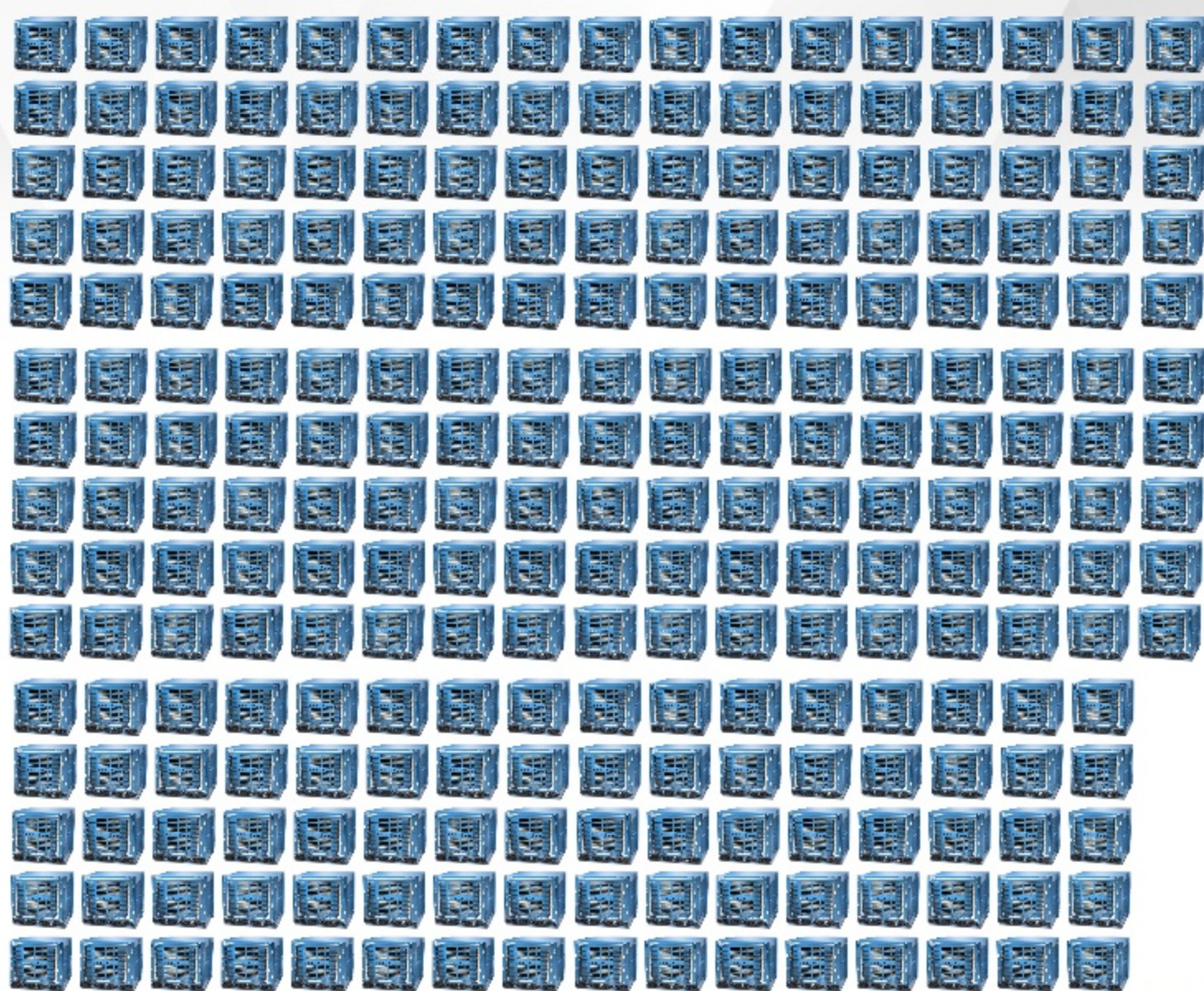


Arista 7508E
1152 x 10GbE
30Tbps backplane
5kW



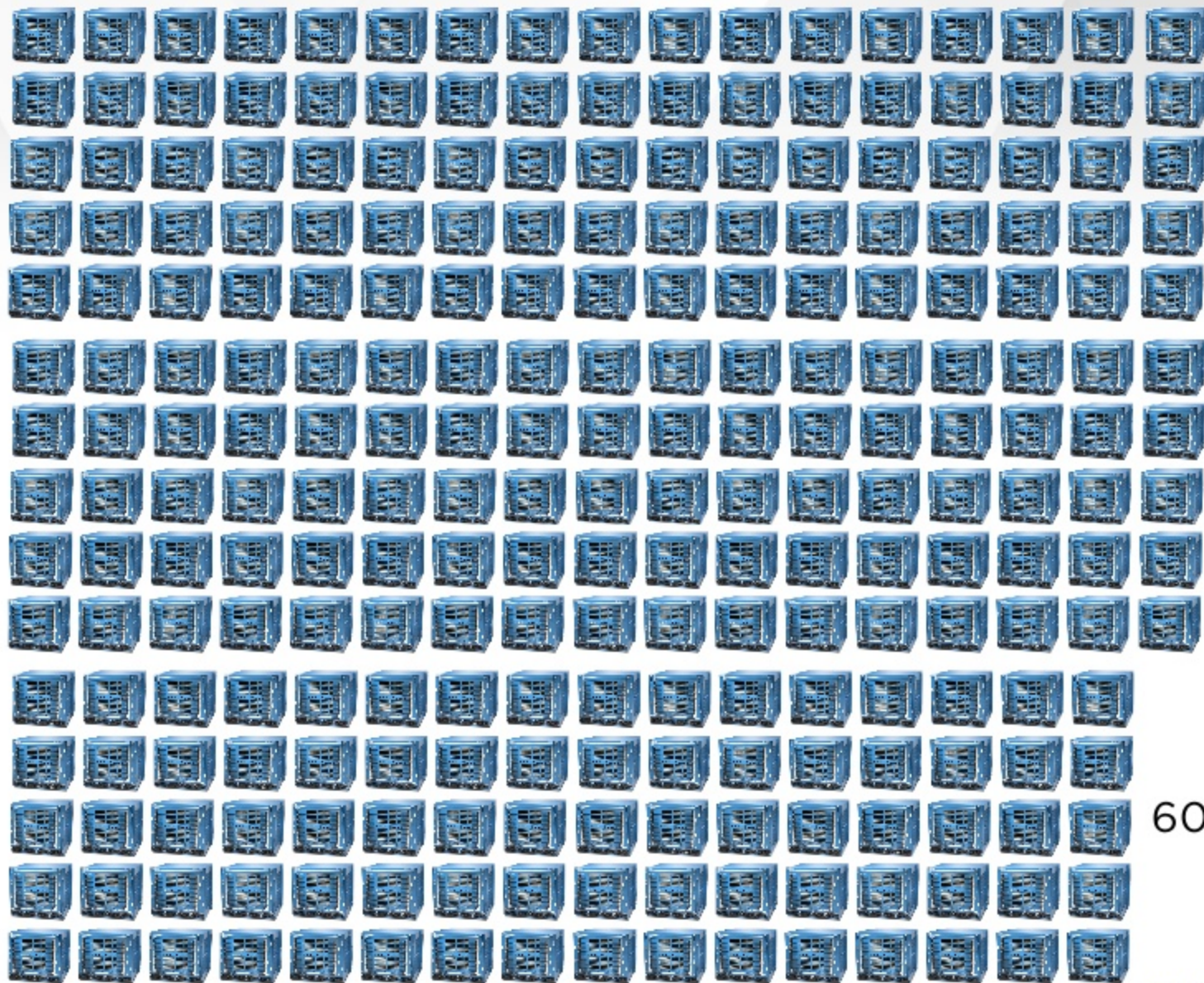
Palo Alto 7050
120Gbps throughput
2.4kW







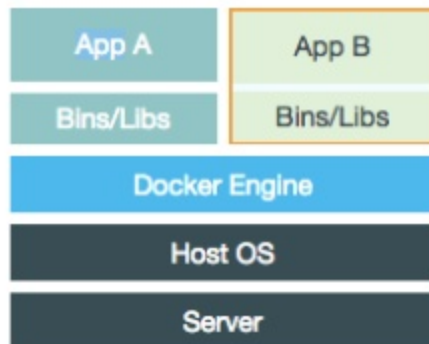
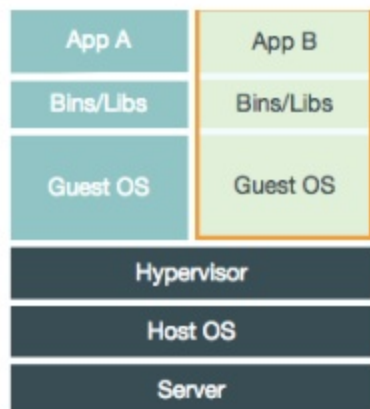
5kW



600kW

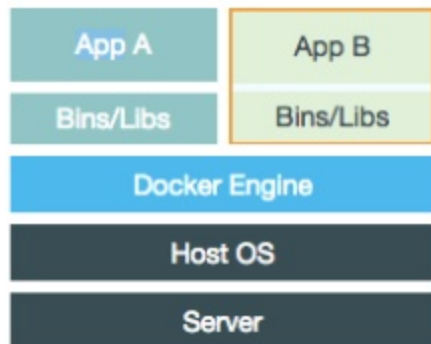
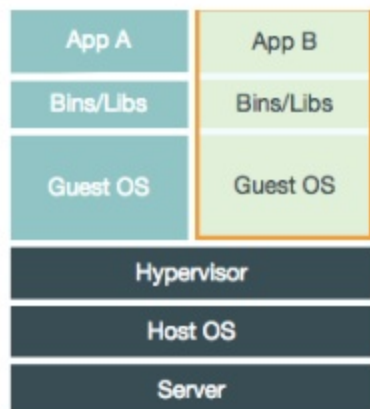
YAHOO!

Containerization collapses the security perimeter



Diagrams from [docker.com](https://www.docker.com)

Containerization collapses the security perimeter

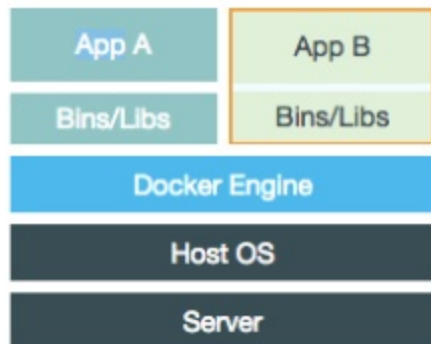
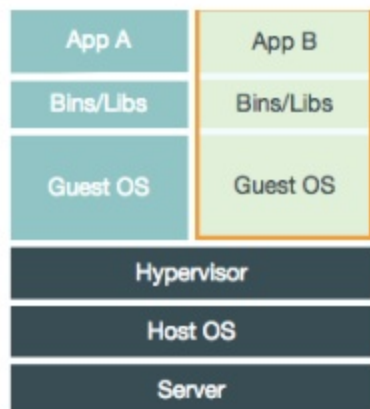


Diagrams from [docker.com](https://docs.docker.com/engine/containers/containers/)

No:

- Virtual soundcard
- Guest OS patching
- VT-x enforcement
- Network controls
- Stable naming
- 1:1 service relationships

Containerization collapses the security perimeter



Diagrams from [docker.com](https://docs.docker.com/engine/containers/containers/)

No:

- Virtual soundcard
- Guest OS patching
- VT-x enforcement
- Network controls
- Stable naming
- 1:1 service relationships

In the long run, this is a good thing!

In the short term, it's a mess to deal with!

The Internet of Unpatchable Crap Things

The screenshot shows the iDevices website with a dark header. The logo 'iDevices' is on the left, followed by navigation links: PLATFORM, APP, BEACON, MODULE, and ABOUT. On the right, there's a 'SHOP OUR PRODUCTS' link with a hamburger menu icon. Below the header, a navigation bar includes 'SHOP', 'iGRILL', 'KITCHEN THERMOMETER', 'iSHOWER²', 'ACCESSORIES', and 'GIFT PACKS'. On the right side of this bar are links for 'MY ACCOUNT', 'ORDER STATUS', and 'VIEW CART'. A promotional banner at the top right states '*FREE US SHIPPING ON \$48+'. The main content area features a large image of a woman smiling in a shower, with a white iShower² device mounted on the wall. To the right of the image, the text reads 'iShower²', 'Your Music. Anytime. Anywhere.', and 'Bluetooth® water-resistant speaker connects to your smart device for anytime listening of your favorite audio apps.' Below this is the price '\$99.99' and two buttons: 'VIEW DETAILS' and 'BUY NOW'. A dark blue banner at the bottom of the main section says 'Free Shipping on Orders Over \$48 or \$5 Flat Rate Shipping'. Below the main section are three smaller product tiles. The first tile shows an iGrill device on a grill with the text 'GET YOUR GRILL ON iGrill'. The second tile shows a Kitchen Thermometer with the text 'SERVE UP PERFECTION Kitchen Thermometer'. The third tile shows a metal band accessory with the text 'EXPAND YOUR SKILLS Accessories'.

iDevices

PLATFORM APP BEACON MODULE ABOUT

SHOP OUR PRODUCTS

SHOP iGRILL KITCHEN THERMOMETER iSHOWER² ACCESSORIES GIFT PACKS

*FREE US SHIPPING ON \$48+

MY ACCOUNT ORDER STATUS VIEW CART

iShower²

Your Music. Anytime. Anywhere.

Bluetooth® water-resistant speaker connects to your smart device for anytime listening of your favorite audio apps.

\$99.99 VIEW DETAILS BUY NOW

Free Shipping on Orders Over \$48 or \$5 Flat Rate Shipping

GET YOUR GRILL ON iGrill

SERVE UP PERFECTION Kitchen Thermometer

EXPAND YOUR SKILLS Accessories

store.iddevices.com

YAHOO!

What AppSec Needs to Accomplish

Apps have to be secure by default

Security Matrix

Spot a mistake? Let us know! We go for fail if unclear - rather too harsh than too lax.

<https://code.google.com/p/mustache-security/>
by cure53.de

Framework	SEC-A	SEC-B	SEC-C	SEC-D	SEC-E	SEC-F
VueJS	Fail	Fail	Fail	Fail	Fail	Fail
AngularJS 1.0.8	Fail	Fail	Fail	Fail	PASS	Fail
AngularJS 1.2.0	Fail	PASS	Fail	Fail	PASS	PASS
CanJS	Fail	Fail	PASS	Fail	Fail	Fail
Underscore.js	Fail	Fail	PASS	Fail	Fail	Fail
KnockoutJS	Fail	Fail	Fail	Fail	Fail	Fail
Ember.js	Fail	PASS	PASS	Fail	PASS	TBD
Polymer	TBD	TBD	TBD	TBD	TBD	TBD
Ractive.js	Fail	Fail	Fail	Fail	Fail	Fail
jQuery	TBD	TBD	TBD	TBD	PASS	TBD
JsRender	Fail	Fail	Fail	Fail	Fail	Fail
Kendo UI	Fail	Fail	Fail	Fail	Fail	Fail

- **SEC-A** Are template expressions executed without using eval or Function? (yes = pass)
- **SEC-B** Is the the execution scope well isolated or sand-boxed? (yes = pass)
- **SEC-C** Can only script elements serve as template containers? (yes = pass)
- **SEC-D** Does the framework allow, encourage or even enforce separation of code and content? (yes = pass)
- **SEC-E** Does the framework maintainer have a security response program? (yes = pass)
- **SEC-F** Does the Framework allow or encourage safe CSP rules to be used (yes = pass)

Apps have to be secure by default

Security Matrix

Spot a mistake? Let us know! We go for fail if unclear - rather too harsh than too lax.

<https://code.google.com/p/mustache-security/>
by [cure53.de](#)

Framework	SEC-A	SEC-B	SEC-C	SEC-D	SEC-E	SEC-F
VueJS	Fail	Fail	Fail	Fail	Fail	Fail
AngularJS 1.0.8	Fail	Fail	Fail	Fail	PASS	Fail
AngularJS 1.2.0	Fail	PASS	Fail	Fail	PASS	PASS
CanJS	Fail	Fail	PASS	Fail	Fail	Fail
Underscore.js	Fail	Fail	PASS	Fail	Fail	Fail
KnockoutJS	Fail	Fail	Fail	Fail	Fail	Fail
Ember.js	Fail	PASS	PASS	Fail	PASS	TBD
Polymer	TBD	TBD	TBD	TBD	TBD	TBD
Ractive.js	Fail	Fail	Fail	Fail	Fail	Fail
jQuery	TBD	TBD	TBD	TBD	PASS	TBD
JsRender	Fail	Fail	Fail	Fail	Fail	Fail
Kendo UI	Fail	Fail	Fail	Fail	Fail	Fail

How many developers understand the security risk they imported?

- SEC-A Are template expressions executed without using eval or Function? (yes = pass)
- SEC-B Is the the execution scope well isolated or sand-boxed? (yes = pass)
- SEC-C Can only script elements serve as template containers? (yes = pass)
- SEC-D Does the framework allow, encourage or even enforce separation of code and content? (yes = pass)
- SEC-E Does the framework maintainer have a security response program? (yes = pass)
- SEC-F Does the Framework allow or encourage safe CSP rules to be used (yes = pass)

App Sec doesn't have to be realtime or inline

- 10Gb Ethernet = 67ns between frames