september 2023

MARK G MURRAY

Executive Speechwriter
+ Creative Director

phone +1.214.354.6482
email connect@markgmurray.com
wordpress markgmurray.com
office Dallas, TX

writing sample

ceo keynote

MWC Keynote for the Chief Executive Officer
Topic: The Foundations of the Digital Transformation

Mobile World Congress 2018 Day One Keynote, *'Aftermarket Afterthought?'*
Tuesday, February 27, 2018 | Barcelona International Convention Centre (CCIB) @ Fira Gran Via
CONTACT—Mark G. Murray, 214-354-6482

EVENT THEME
#BetterFuture

REHEARSAL SCRIPT + GRAPHICS REVIEW | February 23, 2018 | San Francisco, CA

<BEGIN>

Karen Tso Intro—
"Ladies and gentlemen, it's my pleasure to welcome to the MWC stage, Chris Young, CEO of McAfee. But first, let's learn how McAfee answers the cybersecurity challenge all of us face in connecting—and protecting—the mobile world.

...

ROLL ANTHEM VIDEO (1:15)

...

(Chris enters stage right, to demo area)

Cold Open from darkness (4:00)

Live Alexa demo:

CHRIS
"Alexa, launch McAfee."

ALEXA

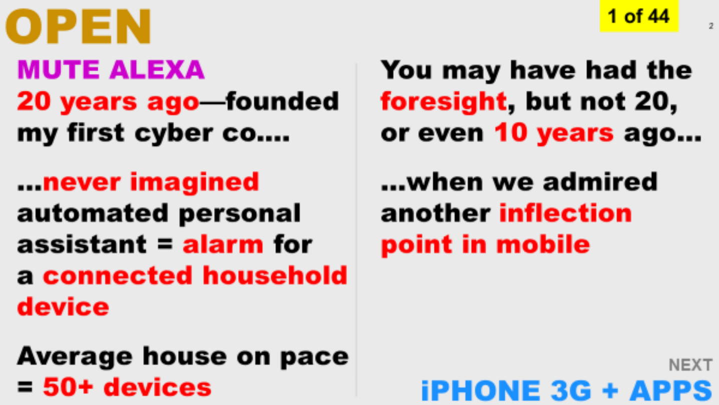
"Welcome to Secure Home Platform. What would you like to do?"

CHRIS
"Read my notifications."

ALEXA
"Okay. Here are your recent notifications. We have just blocked…because it may have been putting you at risk."

...

SLIDE 1—Red McAfee set warmer with white logo



OPEN

1 of 44

MUTE ALEXA

20 years ago—founded my first cyber co….

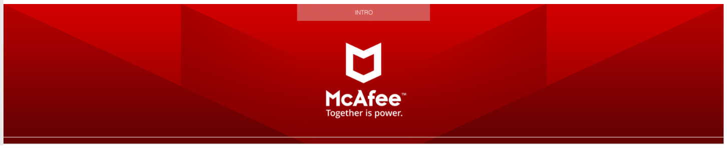
…never imagined automated personal assistant = alarm for a connected household device

Average house on pace = 50+ devices

You may have had the foresight, but not 20, or even 10 years ago…

…when we admired another inflection point in mobile

NEXT
iPHONE 3G + APPS



CHRIS
Twenty years ago, when I started my first cybersecurity company, I would never have imagined a day when an automated personal assistant would sound the alarm of a security alert by way of a connected lightbulb. I also wouldn't have predicted that the average household would have 50 connected devices to manage. Maybe those in this room had this foresight – but likely not a decade ago, when we were admiring another impressive inflection point in this industry.

[SHOULD ALEXA DEMO FAIL]:

Ladies and gentlemen, welcome to the world of live tradeshow demos on a huge stage. It seems there may be interference preventing the demo from working. Being in security, I always think of a Plan B. So, let's go to tape and show you what Alexa can now do with McAfee. [ROLL TAPE]

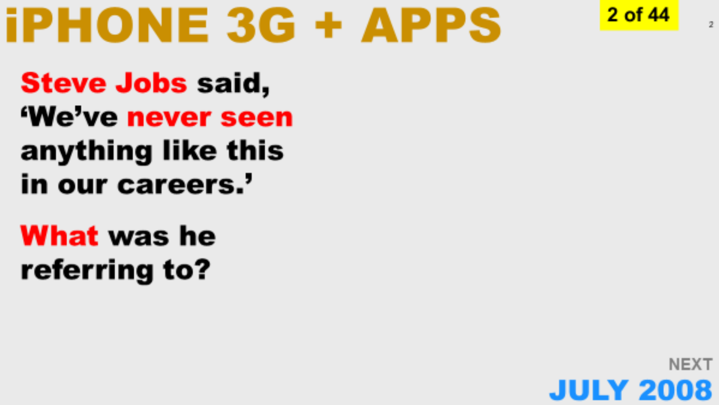
[*Gary: Hi Chris. Thanks for having me at MWC. I'm pleased to welcome you and the audience into my home, where I have a fully connected home network of smart devices. While I may not yet be at the 50 connected devices expected in the average home by 2020, I'm well on my way. Alexa, open McAfee. Read my notifications.*

Alexa: We have detected a vulnerability in the family room light. Now would be a good time to reset the default password to something only you would know.

Gary: Chris, I'll be back with you in a few. Seems I've got a password that needs changing.]

…

SLIDE 2—Steve Jobs



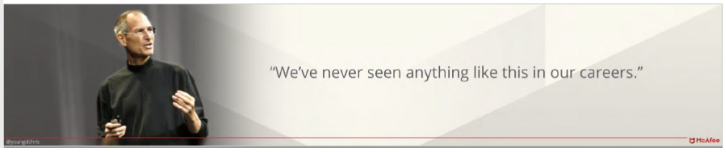
iPHONE 3G + APPS

2 of 44

Steve Jobs said, 'We've never seen anything like this in our careers.'

What was he referring to?

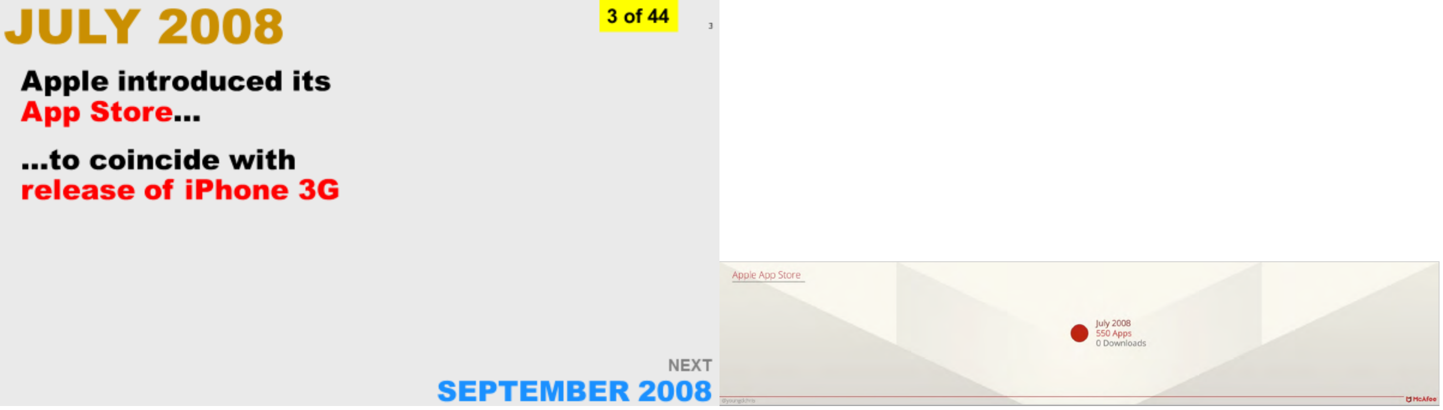
NEXT
JULY 2008



Even Steve Jobs remarked at the time, "We've never seen anything like this in our careers." To what was he referring?

…

SLIDE 3—July 2008



JULY 2008

3 of 44

Apple introduced its
App Store...

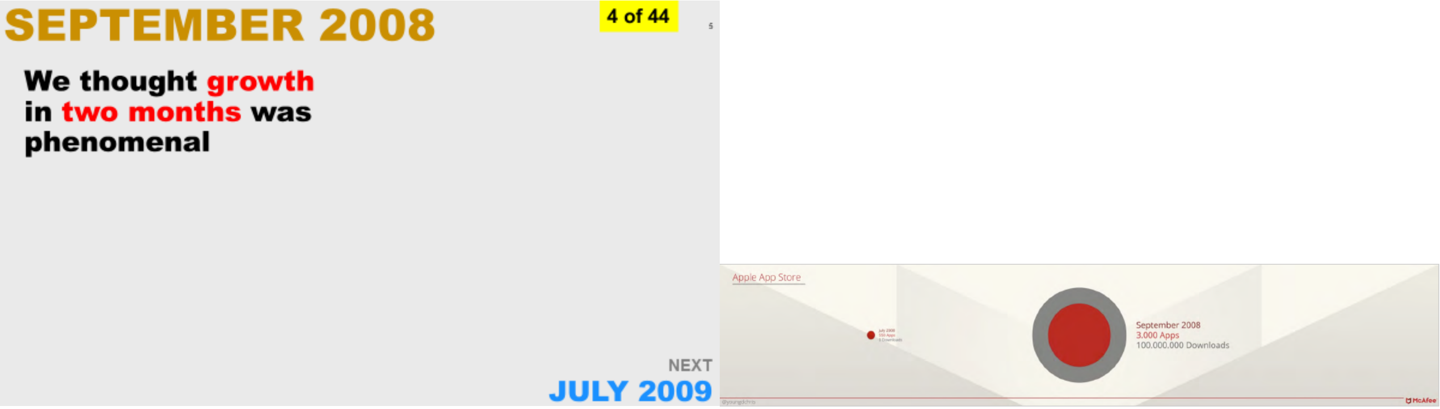
...to coincide with
release of iPhone 3G

NEXT
SEPTEMBER 2008

In July of 2008, Apple introduced its App Store, to coincide with the release of the iPhone 3G.

...

SLIDE 4—(Carousel effect) September 2008



SEPTEMBER 2008

4 of 44

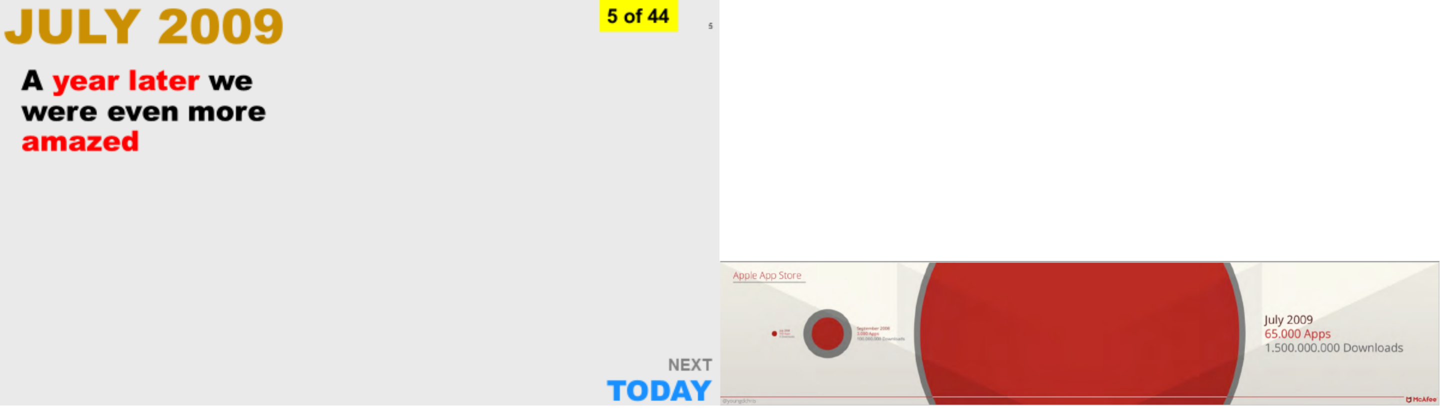
We thought growth
in two months was
phenomenal

NEXT
JULY 2009

We thought the growth within the first two months was astronomical.

...

SLIDE 5—(Carousel effect) July 2009



JULY 2009

5 of 44

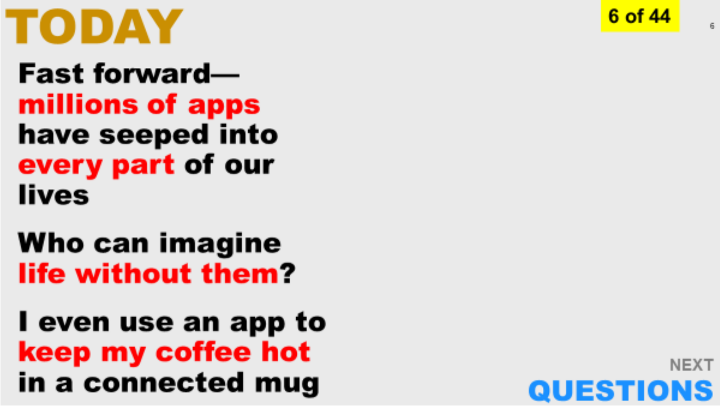
A year later we
were even more
amazed

NEXT
TODAY

A year later we were even more amazed.

...

SLIDE 6—(Carousel effect) Today



TODAY

6 of 44

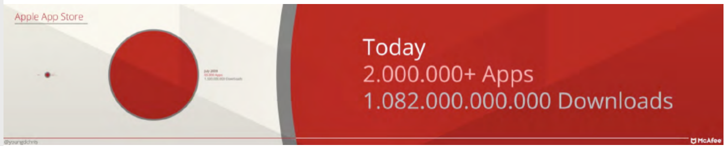
6

Fast forward—
millions of apps
have seeped into
every part of our
lives

Who can imagine
life without them?

I even use an app to
keep my coffee hot
in a connected mug

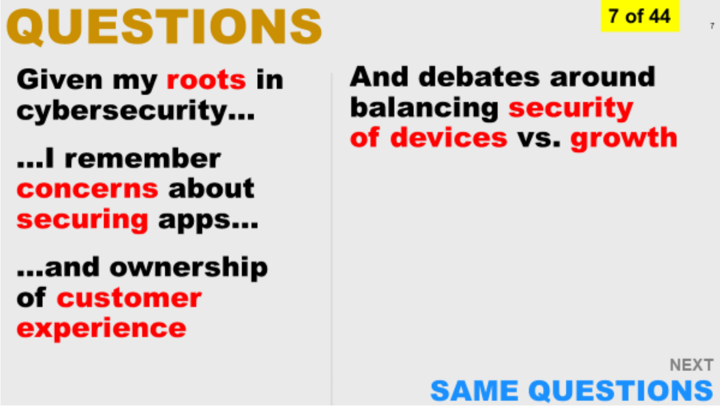
NEXT
QUESTIONS



But fast-forward to today to the millions of apps that have seeped into every part of our lives…and who can imagine life without them? I even have a mobile app to keep my coffee hot in a connected mug.

…

SLIDE 7—Transition to questions



QUESTIONS

7 of 44

7

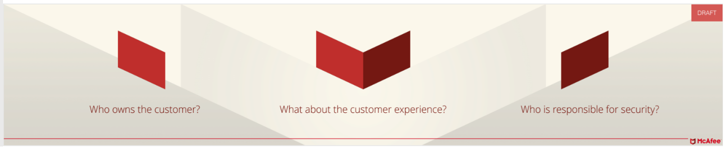
Given my roots in
cybersecurity…

…I remember
concerns about
securing apps…

…and ownership
of customer
experience

And debates around
balancing security
of devices vs. growth

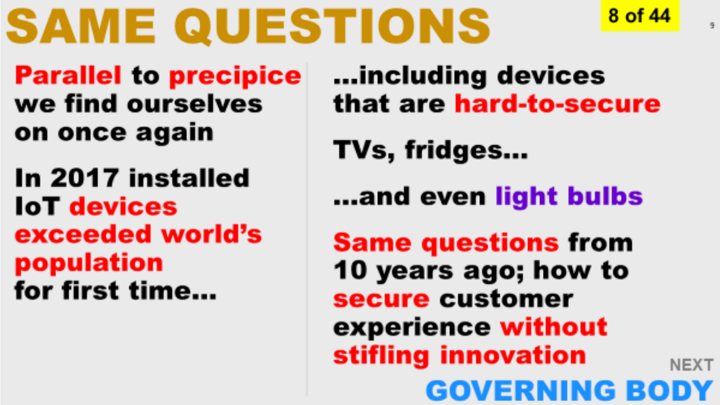
NEXT
SAME QUESTIONS


DRAFT
Who owns the customer?
What about the customer experience?
Who is responsible for security?
McAfee

Given my roots in cybersecurity, I definitely remember concerns about securing the apps in the storefront and ownership of the customer experience. I also recall debates around security versus growth in the category.

…

SLIDE 8—IoT



SAME QUESTIONS

8 of 44

9

Parallel to precipice
we find ourselves
on once again

In 2017 installed
IoT devices
exceeded world's
population
for first time…

…including devices
that are hard-to-secure

TVs, fridges…

…and even light bulbs

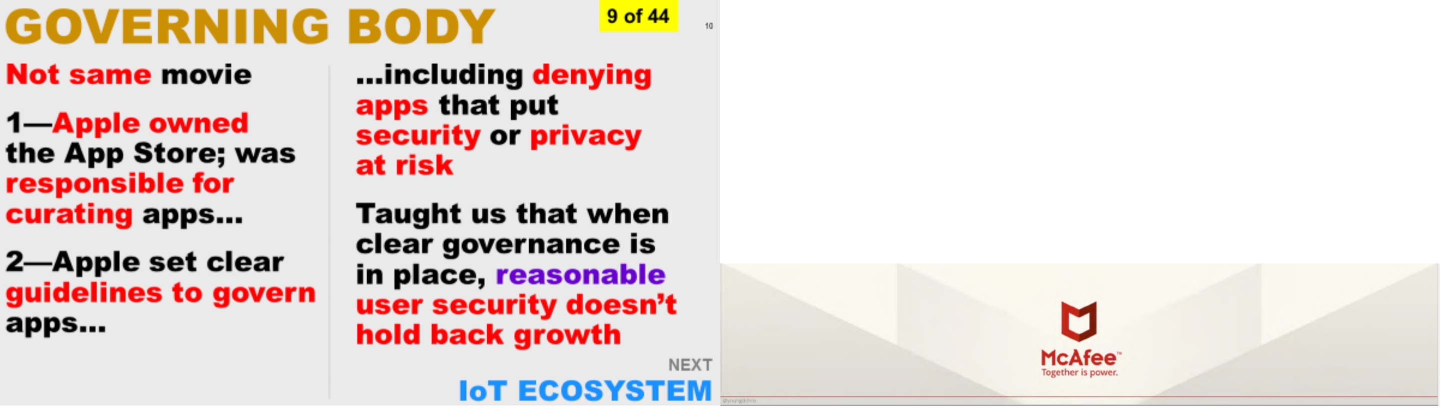
Same questions from
10 years ago; how to
secure customer
experience without
stifling innovation

NEXT
GOVERNING BODY

It resonates with me as an interesting parallel to the precipice we find ourselves on once again. Last year, IoT installed devices – those hard-to-secure items like TVs, fridges, and yes, light bulbs – exceeded the world's population for the first time. And, those same questions we were asking ourselves ten years ago are once again in the forefront, in particular in how we will secure the customer experience without stifling innovation.

...

SLIDE 9—Ivory McAfee set warmer with red logo



GOVERNING BODY

9 of 44

10

Not same movie

1—Apple owned the App Store; was responsible for curating apps...

2—Apple set clear guidelines to govern apps...

...including denying apps that put security or privacy at risk

Taught us that when clear governance is in place, reasonable user security doesn't hold back growth

NEXT

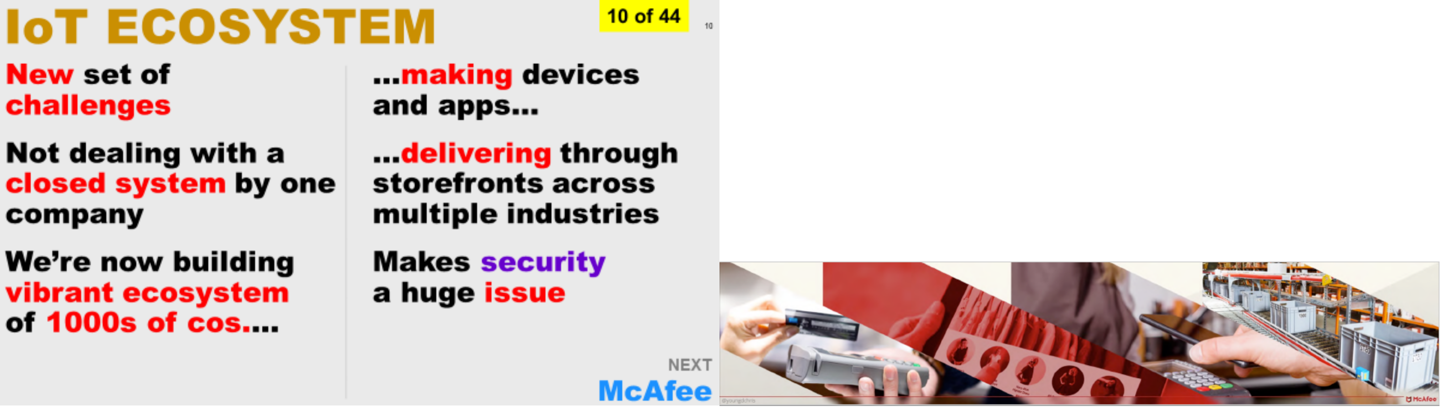
IoT ECOSYSTEM

McAfee
Together is power.

Now, I'm not suggesting we are seeing the exact same movie play out before our eyes. For one, Apple owned the App Store and, as such, was responsible for curating applications – something it does to this day. Apple established clear guidelines to govern which apps would eventually get through – including denying applications that present security or privacy risks. Apple taught us that, when a clear governing body exists, user security can be reasonably upheld without compromising growth.

...

SLIDE 10—Vibrant ecosystem



IoT ECOSYSTEM

10 of 44

10

New set of challenges

Not dealing with a closed system by one company

We're now building vibrant ecosystem of 1000s of cos....

...making devices and apps...

...delivering through storefronts across multiple industries

Makes security a huge issue

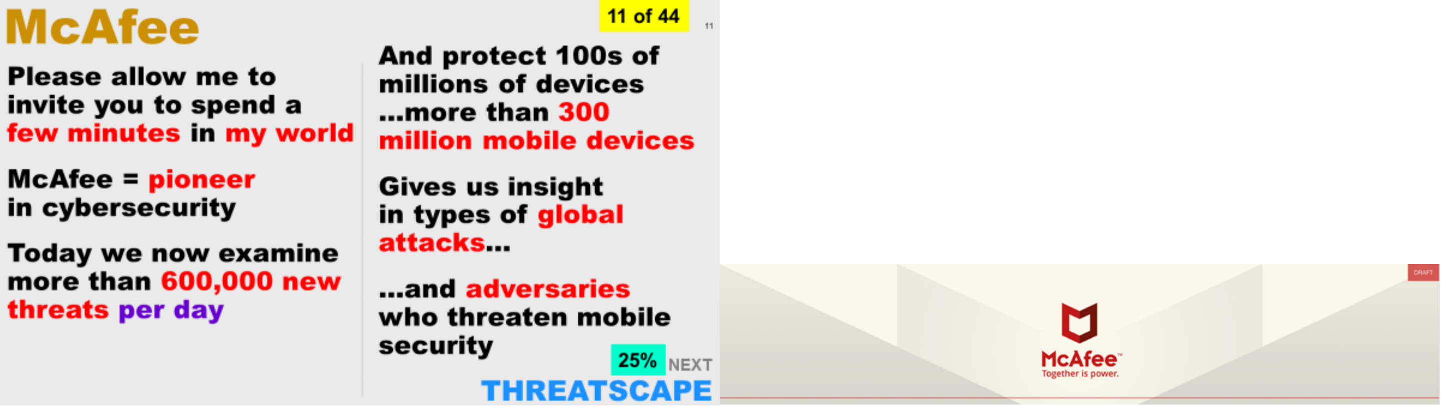
NEXT

McAfee

But, the IoT offers a completely new set of challenges. We're not dealing with a closed system owned by one company. We're building a vibrant ecosystem of thousands of companies making devices and applications and delivering them in storefronts across multiple industries…making security a huge issue

...

SLIDE 11—Ivory McAfee set warmer with red logo + threats and devices stats



McAfee

11 of 44

Please allow me to invite you to spend a few minutes in my world

McAfee = pioneer in cybersecurity

Today we now examine more than 600,000 new threats per day

And protect 100s of millions of devices ...more than 300 million mobile devices

Gives us insight in types of global attacks...

...and adversaries who threaten mobile security

25% NEXT

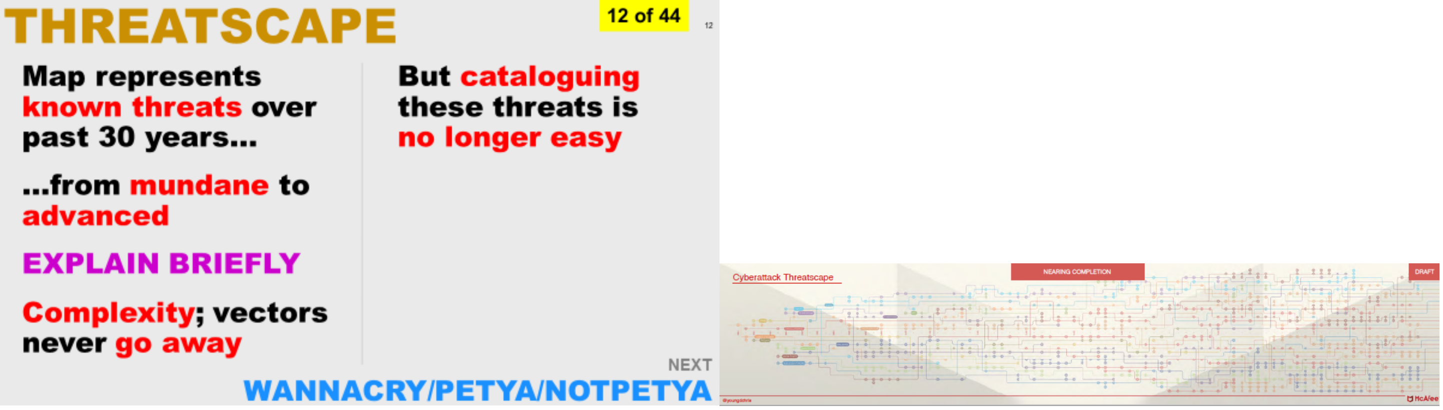
THREATSCAPE

DRAFT
McAfee
Together is power.

Allow me for the next few minutes to take you into my world. McAfee was an early pioneer of cybersecurity. We examine more than 600,000 new threats per *day* and, what's particularly relevant to this audience is that we protect 300 million mobile devices around the world. And that gives us insights into the types of attacks and adversaries who threaten our mobile security.

...

SLIDE 12—Threatscape



THREATSCAPE

12 of 44

Map represents known threats over past 30 years...

...from mundane to advanced

EXPLAIN BRIEFLY

Complexity; vectors never go away

But cataloguing these threats is no longer easy

NEXT

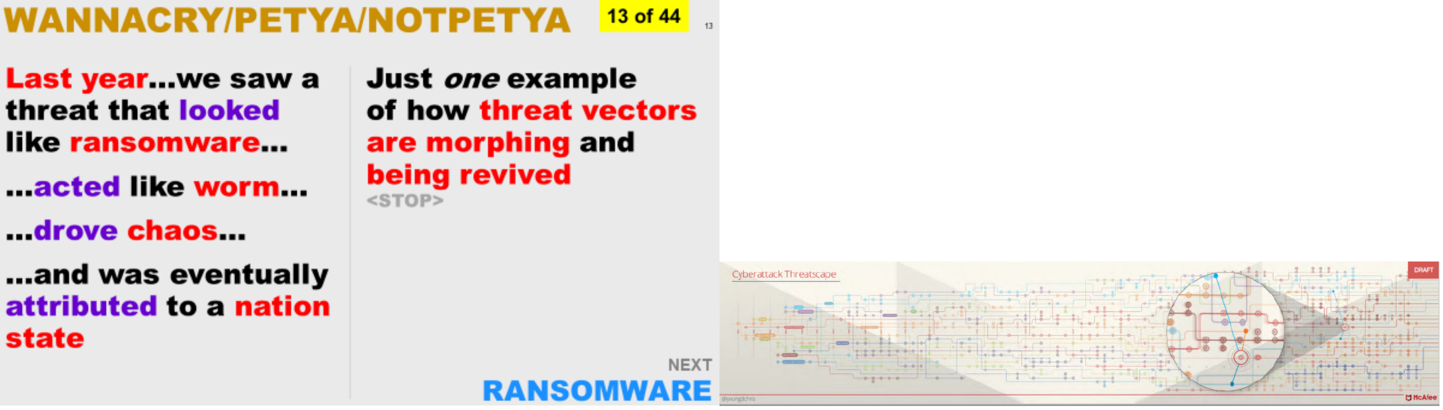
WANNACRY/PETYA/NOTPETYA

Cyberattack Threatscape
NEARING COMPLETION
DRAFT
McAfee

The map behind me represents known threats over the past 30 years, catalogued from the advanced to the mundane. But cataloguing these threats is no longer so easy.

...

SLIDE 13—Threatscape expanded, connecting ransomware + worm + chaos + nation state



WANNACRY/PETYA/NOTPETYA

13 of 44

Last year...we saw a threat that looked like ransomware...

...acted like worm...

...drove chaos...

...and was eventually attributed to a nation state

Just *one* example of how threat vectors are morphing and being revived

<STOP>

NEXT

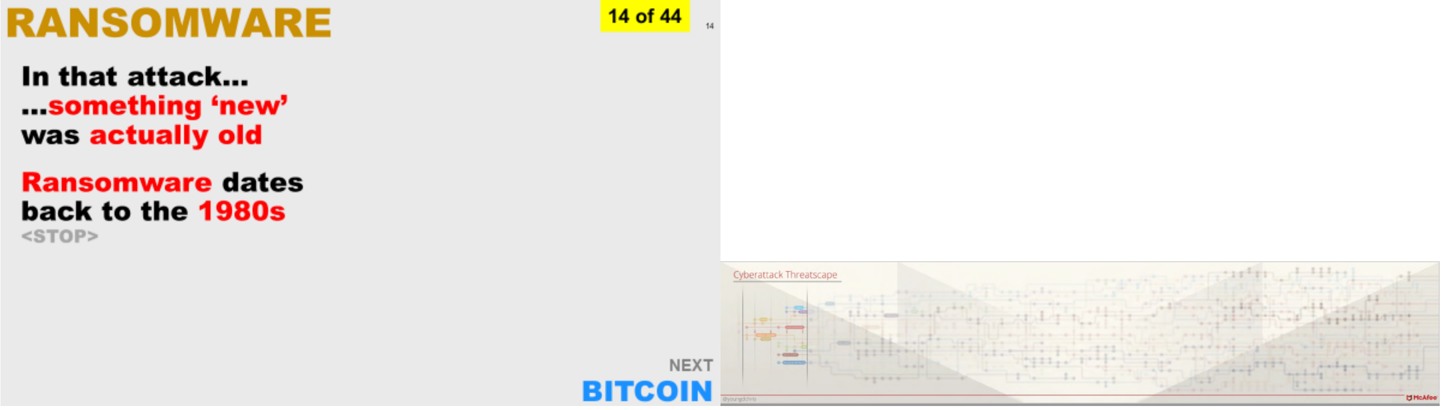
RANSOMWARE

Cyberattack Threatscape
DRAFT
McAfee

Just last year, we saw a threat that looked like ransomware, acted like a worm, drove a ton of chaos and eventually was attributed as a nation-state attack. Just one example of how threat vectors are morphing and being revived.

...

SLIDE 14—Threatscape, 1980s in a moving ‘focus field’



RANSOMWARE

14 of 44

14

In that attack…
…something ‘new’
was actually old

Ransomware dates
back to the 1980s
<STOP>

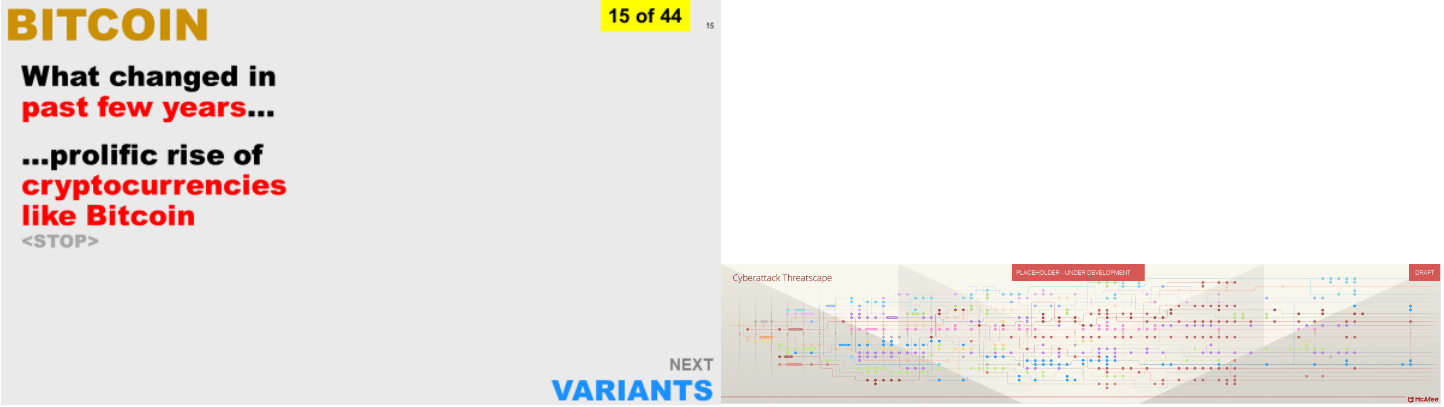
NEXT
BITCOIN

Cyberattack Threatscape
McAfee

For example, in that attack, something that seemed new – ransomware – was something old, dating back to the late 1980s.

…

SLIDE 15—Threatscape, Bitcoin in a moving ‘focus field’



BITCOIN

15 of 44

15

What changed in
past few years…

…prolific rise of
cryptocurrencies
like Bitcoin
<STOP>

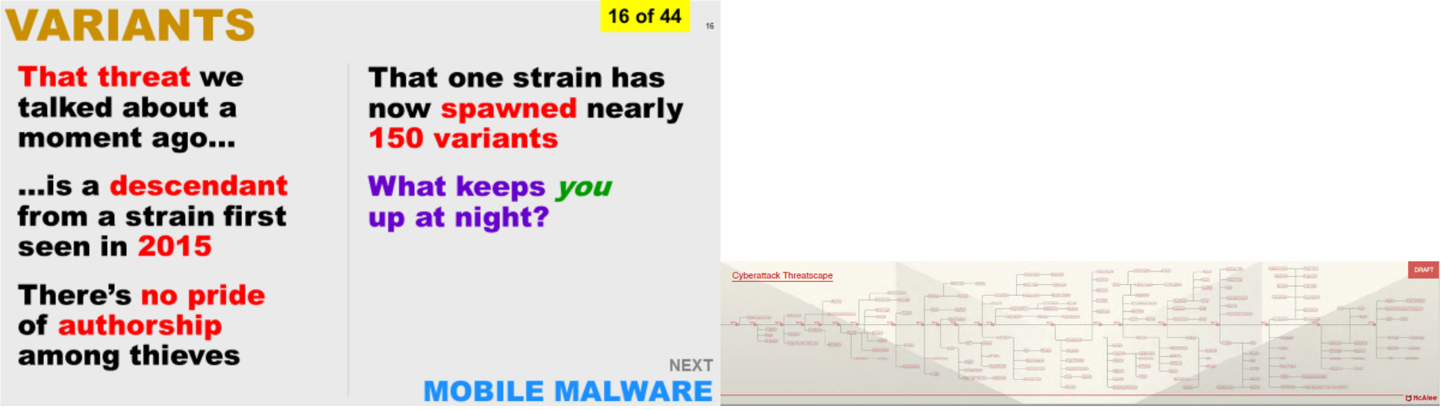
NEXT
VARIANTS

Cyberattack Threatscape
PLACEHOLDER - UNDER DEVELOPMENT
DRAFT
McAfee

What’s changed in the past few years to make ransomware so prolific is the rise of cryptocurrencies, like Bitcoin.

…

SLIDE 16—Threatscape, build-out of WannaCry/Petya families (from HiddenTear in 2015)



VARIANTS

16 of 44

16

That threat we
talked about a
moment ago…

…is a descendant
from a strain first
seen in 2015

There’s no pride
of authorship
among thieves

That one strain has
now spawned nearly
150 variants

What keeps *you*
up at night?

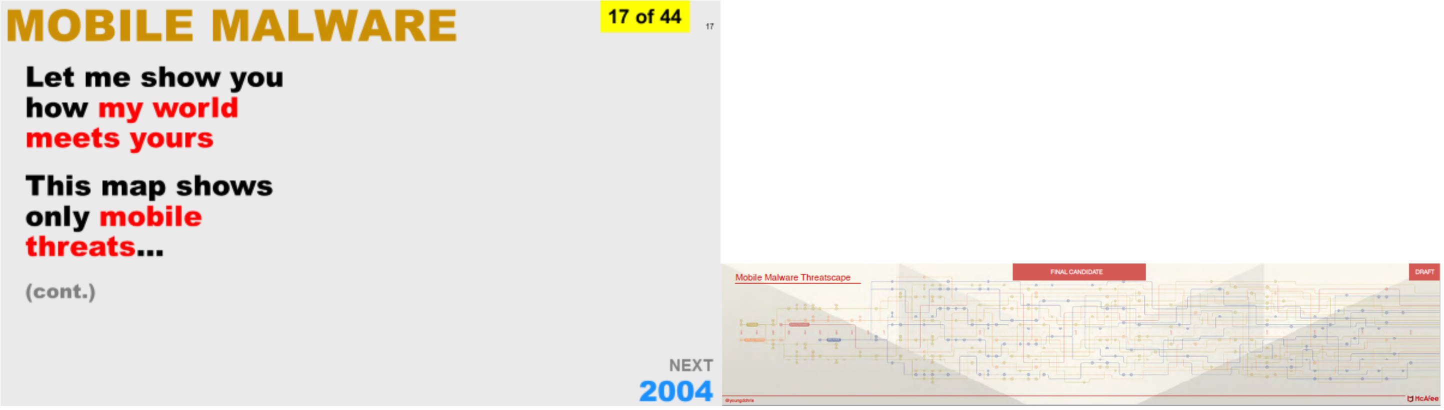
NEXT
MOBILE MALWARE

Cyberattack Threatscape
DRAFT
McAfee

And since there’s no pride of ownership among thieves, that one strain of ransomware has now spawned nearly 150 variants. So, what keeps you up at night? **[SET PIECE: WANNACRY/PETYA RANSOMWARE STRAINS]** That’s a small glimpse into my world.

…

SLIDE 17—Threatscape, mobile malware



MOBILE MALWARE

17 of 44

17

Let me show you how my world meets yours

This map shows only mobile threats…

(cont.)

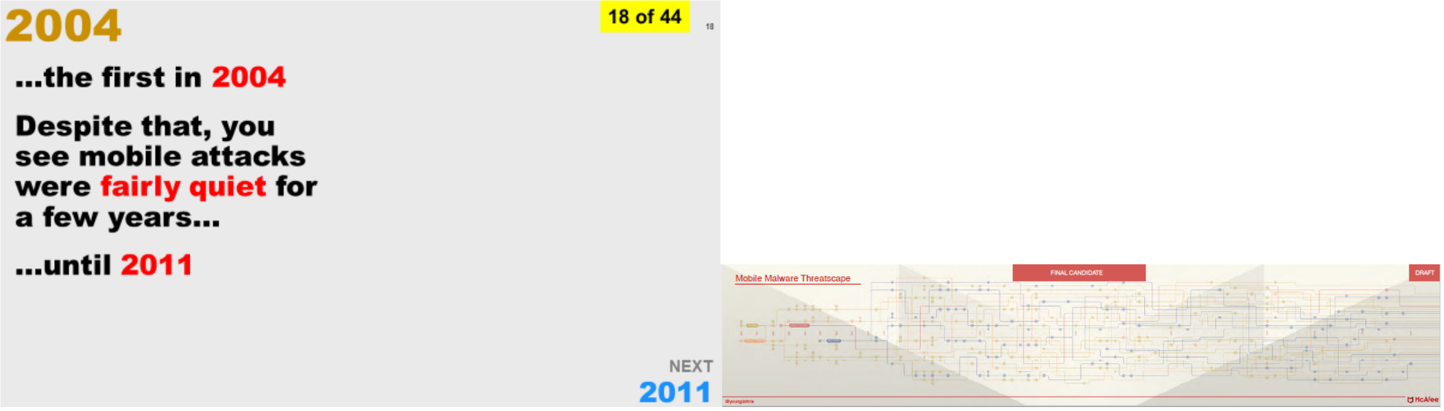
NEXT

2004

Now, let me show you how my world meets yours. This graph shows only mobile threats, the first of which hit the scene in 2004. Despite that, you see that mobile attacks were fairly quiet for several years – until 2011.

…

SLIDE 18—2004



2004

18 of 44

18

…the first in 2004

Despite that, you see mobile attacks were fairly quiet for a few years…

…until 2011

NEXT

2011

…the first in 2004. Despite that, you see mobile attacks were fairly quiet for a few years…until 2011.

…

SLIDE 19—2011

2011

19 of 44

19

Which is when GSMA reports that smartphones hit critical mass in developed world

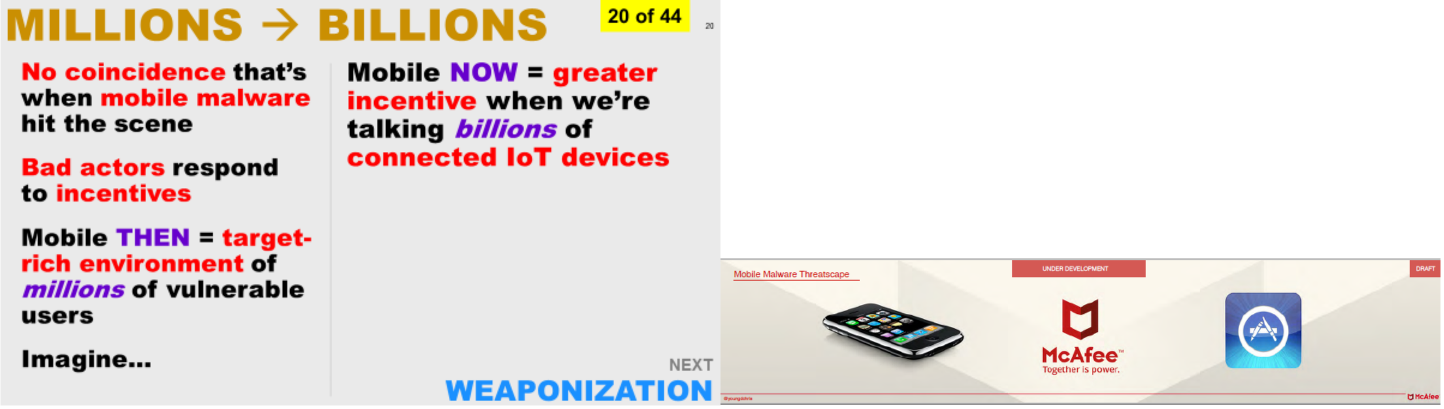
NEXT

MILLIONS → BILLIONS

Which is when GSMA reports that smartphones accounted for 30% of total mobile connections in developed countries.

…

SLIDE 20—3G + App Store



MILLIONS → BILLIONS

20 of 44

No coincidence that's when mobile malware hit the scene

Bad actors respond to incentives

Mobile THEN = target-rich environment of *millions* of vulnerable users

Imagine...

Mobile NOW = greater incentive when we're talking *billions* of connected IoT devices

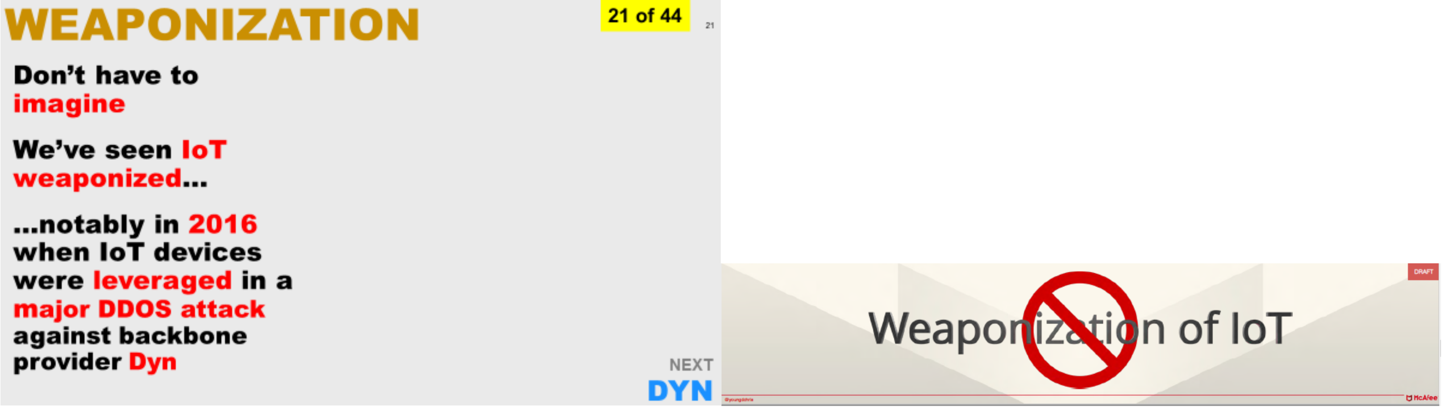
NEXT
WEAPONIZATION

20
Mobile Malware Threatscape
UNDER DEVELOPMENT
DRAFT
McAfee
Together is power.

Not coincidentally, that's also when mobile malware truly it the scene. When bad actors have incentive, they respond. And few things offer greater incentive than a target-rich environment of *millions* of vulnerable users. Imagine how much greater the incentive when we're talking about *billions* of connected IoT devices.

...

SLIDE 21—Weaponization of the IoT



WEAPONIZATION

21 of 44

Don't have to imagine

We've seen IoT weaponized...

...notably in 2016 when IoT devices were leveraged in a major DDOS attack against backbone provider Dyn

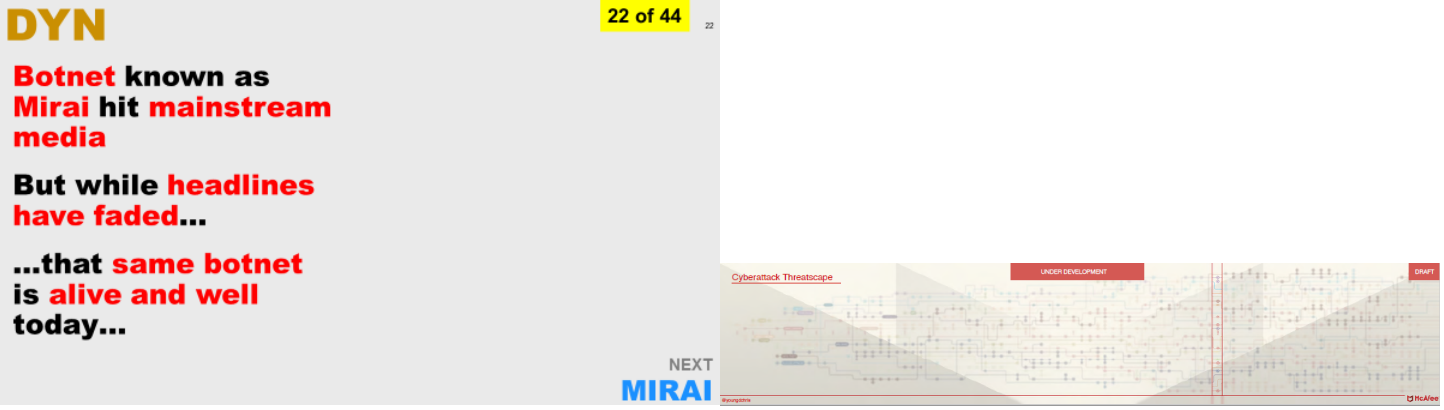
NEXT
DYN

21
DRAFT
Weaponization of IoT

Of course, we don't have to use our imaginations. We've seen the IoT weaponized, most notably in 2016, when IoT devices were leveraged in a major denial-of-service attack against backbone provider Dyn.

...

SLIDE 22—Threatscape + Dyn attack



DYN

22 of 44

Botnet known as Mirai hit mainstream media

But while headlines have faded...

...that same botnet is alive and well today...

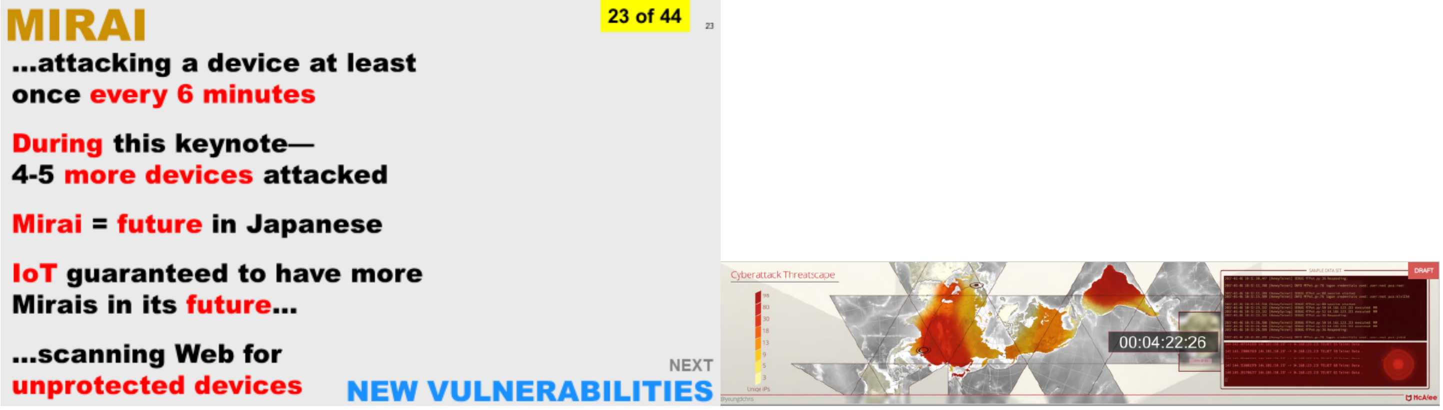
NEXT
MIRAI

22
Cyberattack Threatscape
UNDER DEVELOPMENT
DRAFT

The botnet known as Mirai hit the mainstream media. But, while the headlines have faded that same botnet is alive and well…

...

SLIDE 23—Mirai botnet



MIRAI

23 of 44

…attacking a device at least once every 6 minutes

During this keynote—
4-5 more devices attacked

Mirai = future in Japanese

IoT guaranteed to have more Mirais in its future…

…scanning Web for unprotected devices

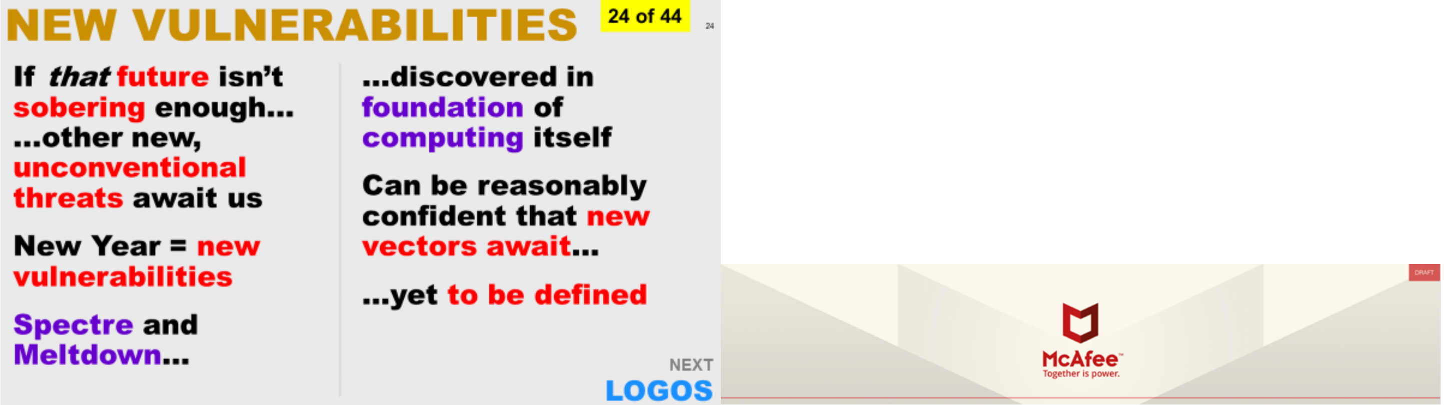
NEXT
NEW VULNERABILITIES

…attacking a new device at least once every six minutes. The word “Mirai” means “future” in Japanese. And, indeed, the IoT is guaranteed to have more Mirais in its future – botnets scanning the Web for unprotected IoT drones.

…

SLIDE 24—Ivory McAfee set warmer with red logo

And, if the certainty of that future isn’t sufficiently sobering, we can be sure other unconventional threats await us. We rang in a new year with the announcement of the Spectre and Meltdown vulnerabilities, which were discovered within the foundation of computing itself. We can be reasonably confident that new threat vectors await, yet to be defined.



NEW VULNERABILITIES

24 of 44

If *that* future isn’t sobering enough…
…other new, unconventional threats await us

New Year = new vulnerabilities

Spectre and Meltdown…

…discovered in foundation of computing itself

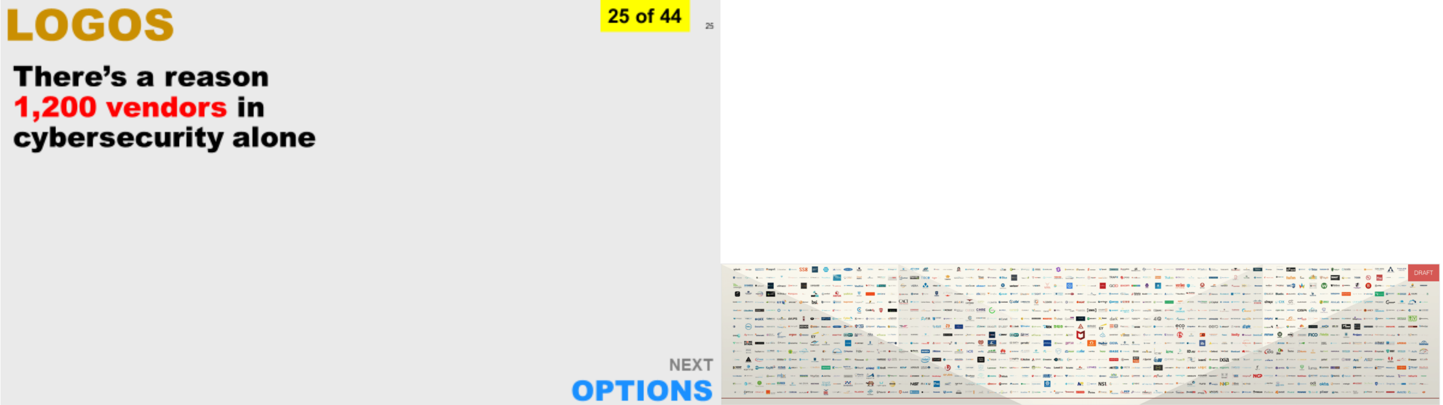
Can be reasonably confident that new vectors await…

…yet to be defined

NEXT
LOGOS

…

SLIDE 25—Universe of logos (McAfee logo shrinks back from the set warmer to join the broader ecosystem)



LOGOS

25 of 44

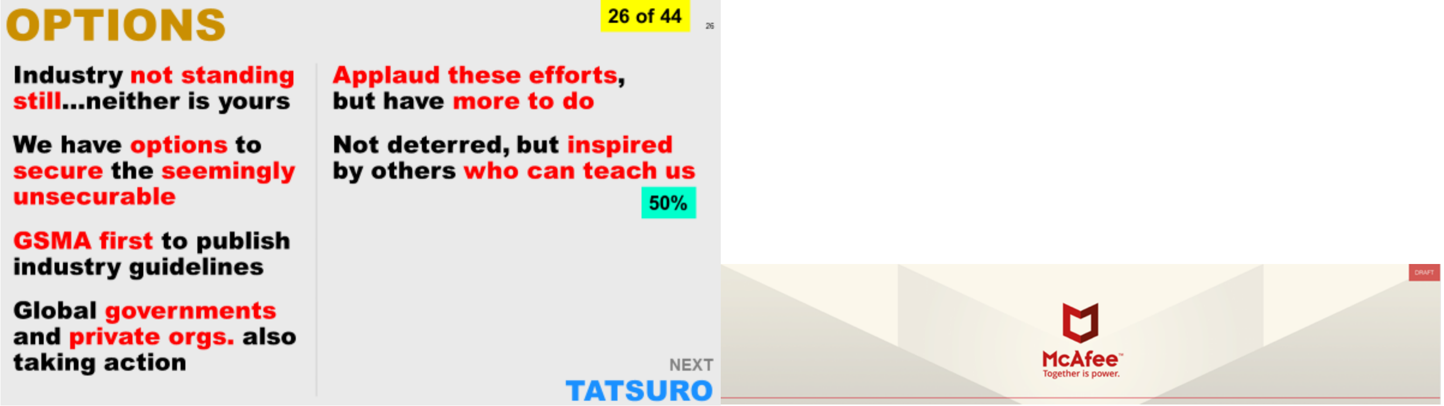
There’s a reason 1,200 vendors in cybersecurity alone

NEXT
OPTIONS

There’s a reason there are 1,200 in the cybersecurity industry alone.

…

SLIDE 26— Ivory McAfee set warmer with red logo



OPTIONS

26 of 44

Industry **not standing still**...neither is yours

We have **options** to **secure** the **seemingly unsecurable**

GSMA first to publish industry guidelines

Global **governments** and **private orgs.** also taking action

Applaud these efforts, but have **more to do**

Not deterred, but **inspired** by others **who can teach us**

50%

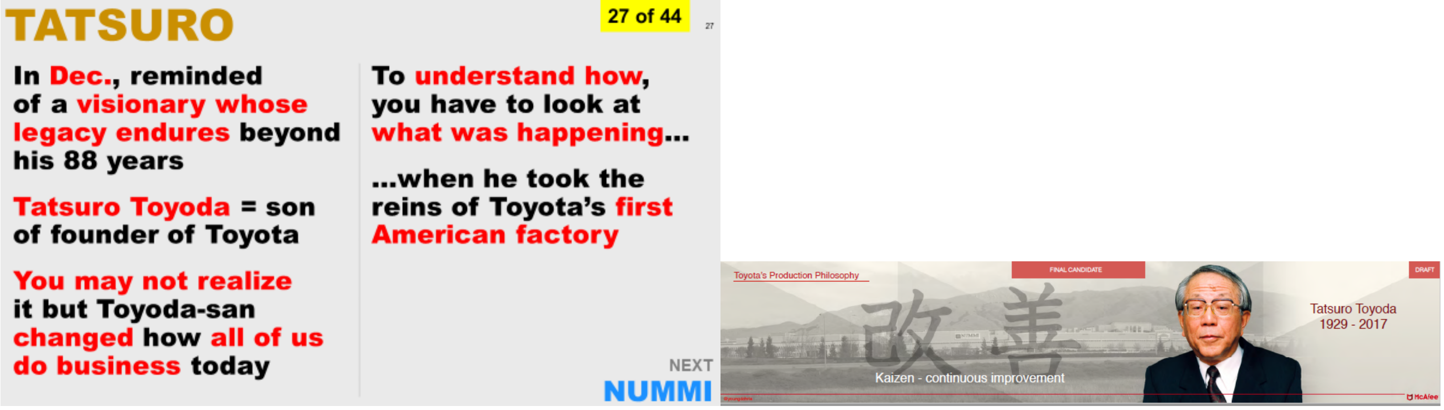
NEXT
TATSURO

And none of us are standing still. There are several options on the table to secure the seemingly unsecurable. One is being led by the GSMA itself – one of the first industry associations to publish guidelines, best practices and a self-assessment around securing the IoT. Around the world, governments and private organizations are tackling the same.

I want to applaud these efforts across the ecosystem. But, we have far to go to stop the greatest existential threat to our digital freedom – cyberattacks – from turning the IoT into the Internet of Terror. I'm not deterred by the challenge. Rather, I'm inspired by others who can teach us how to approach it.

...

SLIDE 27—Tatsuro + kaizen



TATSURO

27 of 44

In **Dec.**, reminded of a **visionary whose legacy endures** beyond his 88 years

Tatsuro Toyoda = son of founder of Toyota

You may not realize it but Toyoda-san **changed** how **all of us do business** today

To **understand how**, you have to look at **what was happening...**

...when he took the reins of Toyota's **first American factory**

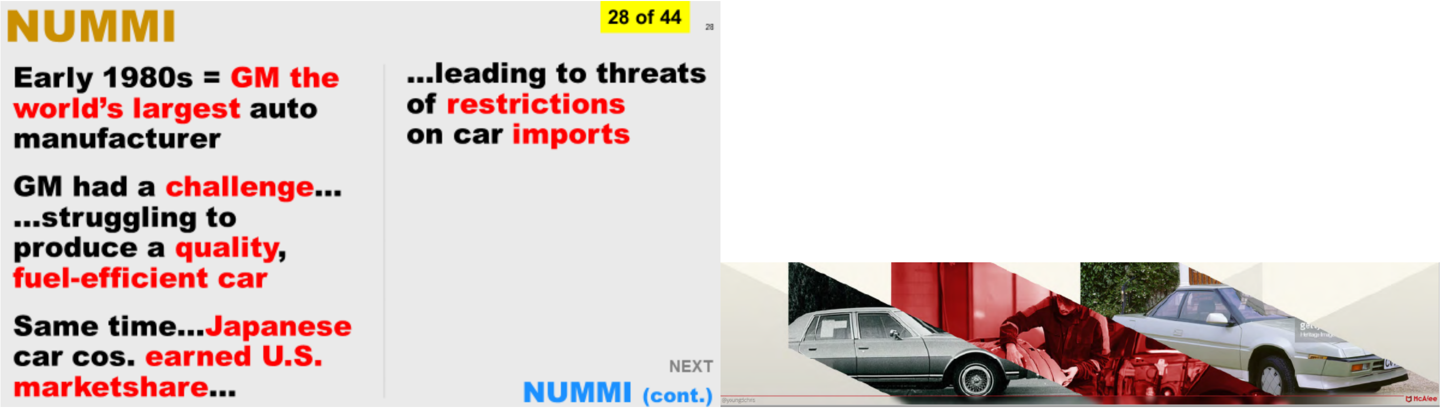
NEXT
NUMMI

Toyota's Production Philosophy
FINAL CANDIDATE
DRAFT
改善
Kaizen - continuous improvement
Tatsuro Toyoda
1929 - 2017
McAfee

In December, I was reminded of a visionary who left a legacy that will endure far beyond his 88 years: Tatsuro Toyoda, son of the founder of the automotive company Toyota. You may not realize it, but Toyoda-san changed the way we all do business today. To understand how, you have to take a look at what was happening at the time he took the reins for his company's first American factory.

...

SLIDE 28—NUMMI parallelograms



NUMMI

28 of 44

Early 1980s = GM the world's largest auto manufacturer

GM had a challenge... ...struggling to produce a quality, fuel-efficient car

Same time...Japanese car cos. earned U.S. marketshare...

...leading to threats of restrictions on car imports

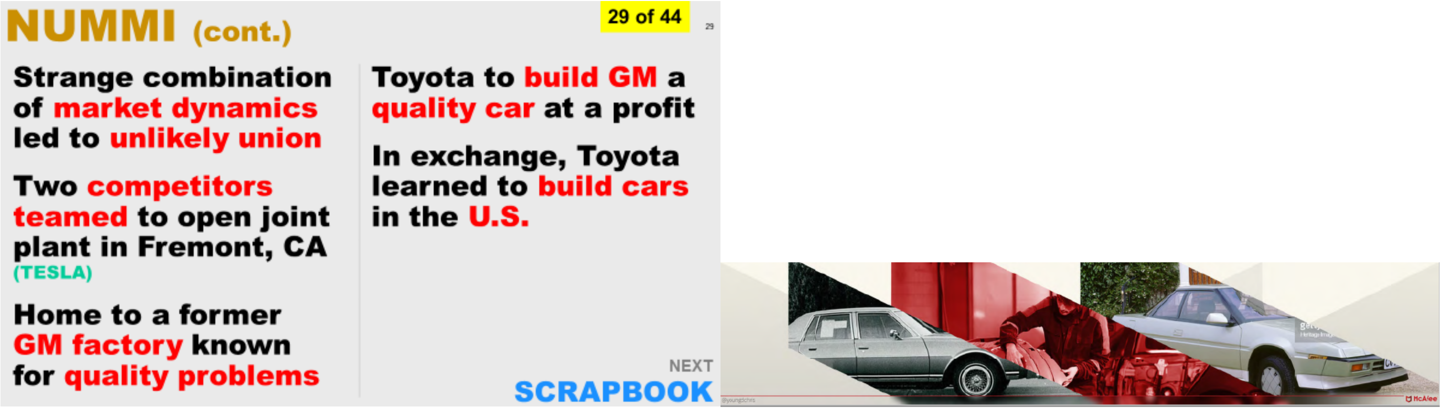
NEXT

NUMMI (cont.)

It was the early 1980s. General Motors, the world's largest car company at the time, had a challenge: it was struggling to produce a quality, fuel-efficient car. At the same time, Japanese car companies were starting to grab US market share – so much so that the US Congress was threatening to restrict car imports.

...

SLIDE 29—NUMMI parallelograms (cont.)



NUMMI (cont.)

29 of 44

Strange combination of market dynamics led to unlikely union

Two competitors teamed to open joint plant in Fremont, CA (TESLA)

Home to a former GM factory known for quality problems

Toyota to build GM a quality car at a profit

In exchange, Toyota learned to build cars in the U.S.

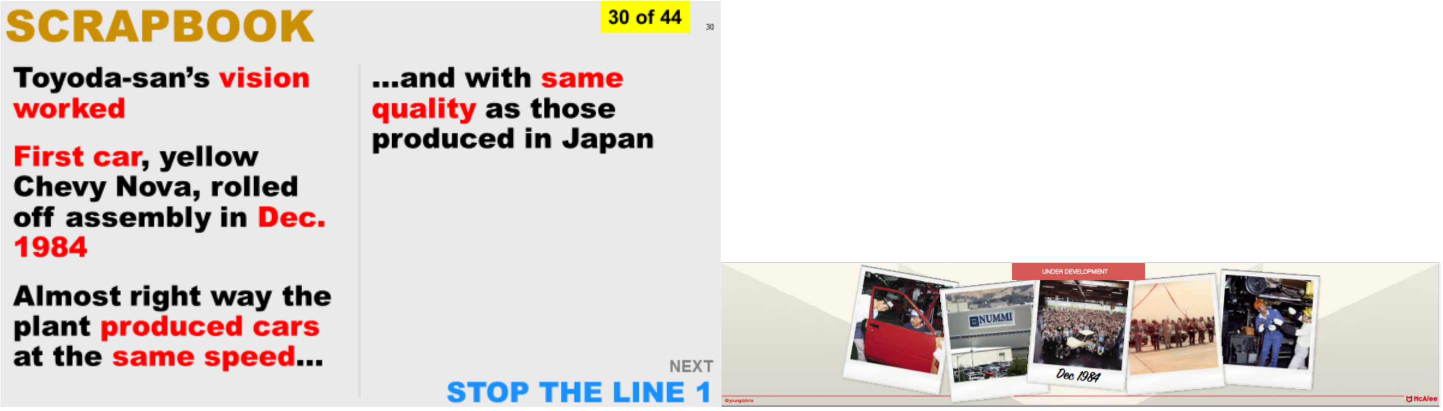
NEXT

SCRAPBOOK

This strange combination of market dynamics led to the unlikeliest of unions. These two competitors teamed up to open a joint plant in Fremont, CA (Tesla), home to a former GM plant that had quality problems. Toyota would build GM a quality small car that would finally turn a profit. In exchange, Toyota would learn to build cars in the US.

...

SLIDE2 30—Yellow Chevy Nova 'Polaroid' (from a Fremont 'scrapbook')



SCRAPBOOK

30 of 44

Toyoda-san's vision worked

First car, yellow Chevy Nova, rolled off assembly in Dec. 1984

Almost right way the plant produced cars at the same speed...

...and with same quality as those produced in Japan

NEXT

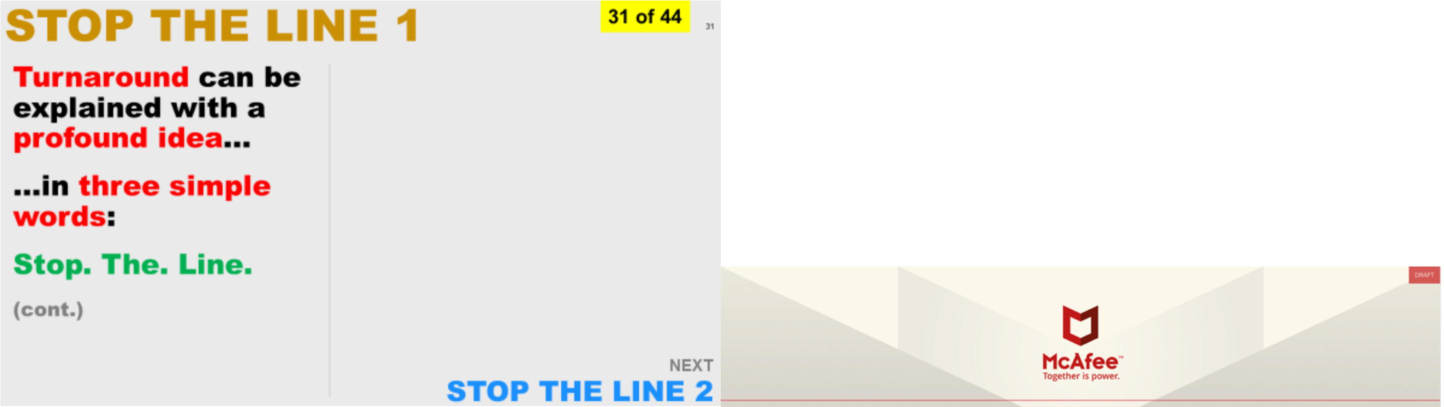
STOP THE LINE 1

UNDER DEVELOPMENT
NUMMI
Dec 1984

Toyoda-san's vision worked. The first car, a yellow Chevy Nova, rolled off the assembly line in December of 1984. And, almost right away, the plant was producing cars at the same speed and with as few defects as those produced in Japan

…

SLIDE 31—Red logo



STOP THE LINE 1

31 of 44

Turnaround can be explained with a profound idea…

…in three simple words:

Stop. The. Line.

(cont.)

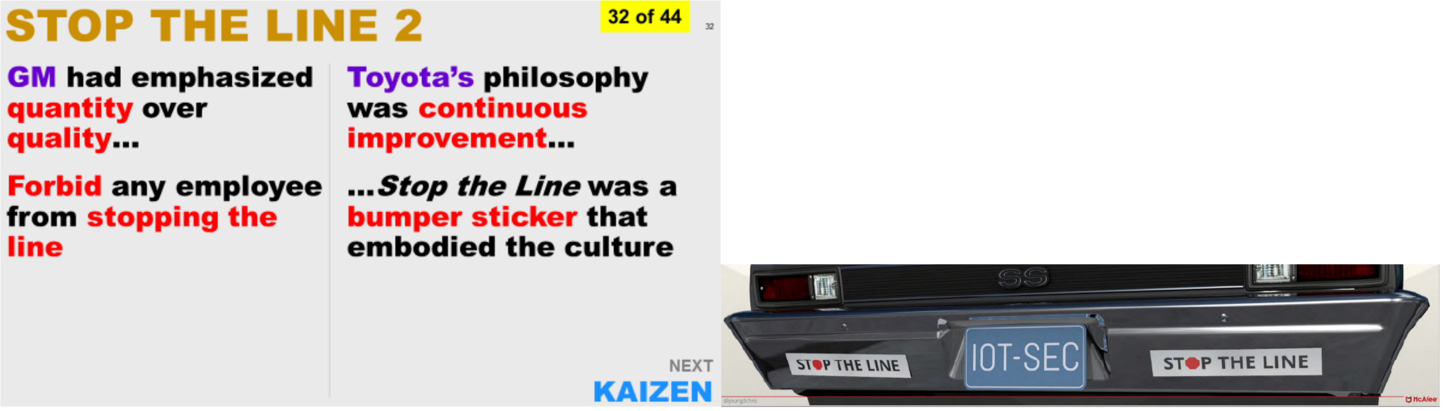
NEXT

STOP THE LINE 2

The turnaround could be explained with a profound idea wrapped in three simple words, “Stop the Line”.

…

SLIDE 32—Bumper stickers



STOP THE LINE 2

32 of 44

GM had emphasized quantity over quality…

Forbid any employee from stopping the line

Toyota’s philosophy was continuous improvement…

…*Stop the Line* was a bumper sticker that embodied the culture

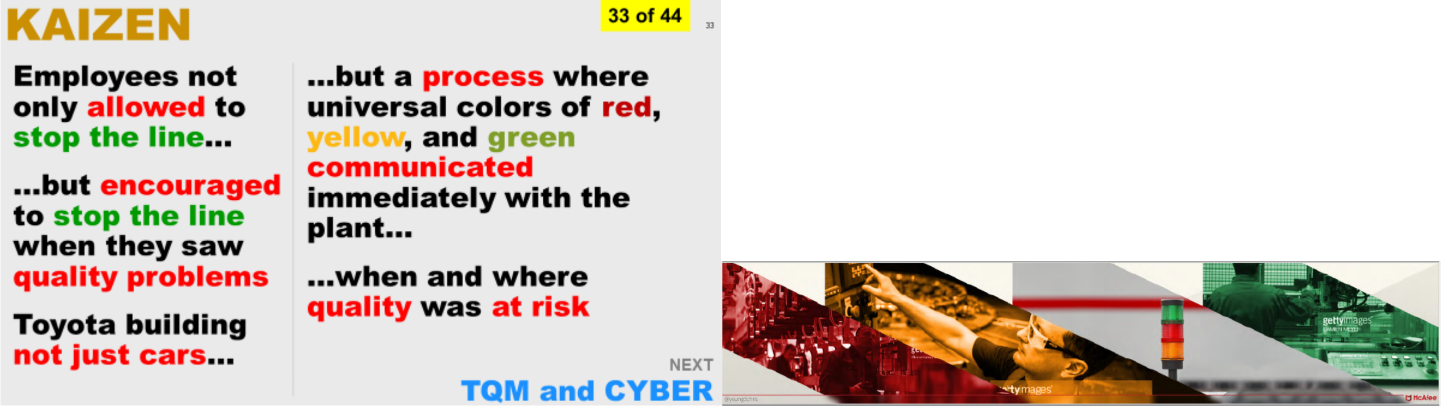
NEXT

KAIZEN

In contrast to GM’s philosophy of emphasizing quantity over quality – one that forbid any employee from stopping the manufacturing line – Toyota built its philosophy on continuous improvement. “Stop the Line” was the bumper sticker slogan that embodied the culture.

…

SLIDE 33—Kaizen parallelograms



KAIZEN

33 of 44

Employees not only allowed to stop the line…

…but encouraged to stop the line when they saw quality problems

Toyota building not just cars…

…but a process where universal colors of red, yellow, and green communicated immediately with the plant…

…when and where quality was at risk

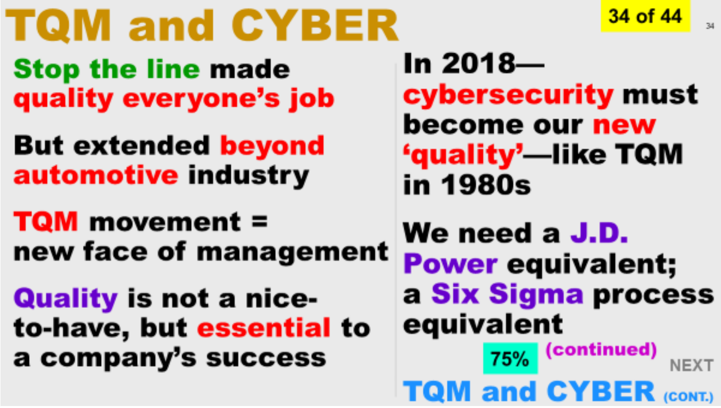
NEXT

TQM and CYBER

Not only were employees allowed to stop the production line when they saw quality problems, they were encouraged to do so. Toyota wasn’t just building cars; they were building a process – one where the universal colors of red, yellow and green immediately communicated to all in the plant where quality was at risk.

...

SLIDE 34—Ivory McAfee set warmer with red logo?



34 of 44

34

TQM and CYBER

Stop the line made quality everyone's job

But extended beyond automotive industry

TQM movement = new face of management

Quality is not a nice-to-have, but essential to a company's success

In 2018—cybersecurity must become our new 'quality'—like TQM in 1980s

We need a J.D. Power equivalent; a Six Sigma process equivalent

75% (continued)

NEXT

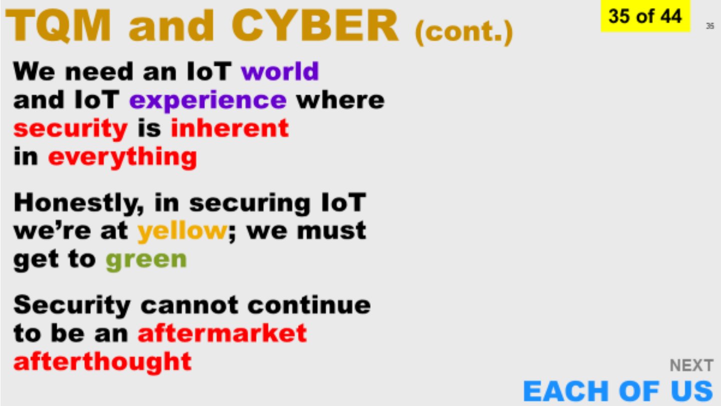
TQM and CYBER (CONT.)

This "Stop the Line" philosophy made quality an inherent part of everyone's job, with impacts that extended far beyond the automotive industry. The Total Quality Management, or TQM, movement was on – where continuous improvement became the new face of management and quality the prize. We learned that quality wasn't a nice-to-have; it was essential to a company's long-term success.

In 2018, I would argue that cybersecurity must become our new quality. We need a security movement – the same way TQM was the quality movement of the 1980s. We need a JD Power equivalent that rewards strong security. We need a Six Sigma process equivalent for security.

...

SLIDE 35—Ivory McAfee set warmer with red logo



35 of 44

35

TQM and CYBER (cont.)

We need an IoT world and IoT experience where security is inherent in everything

Honestly, in securing IoT we're at yellow; we must get to green

Security cannot continue to be an aftermarket afterthought

NEXT

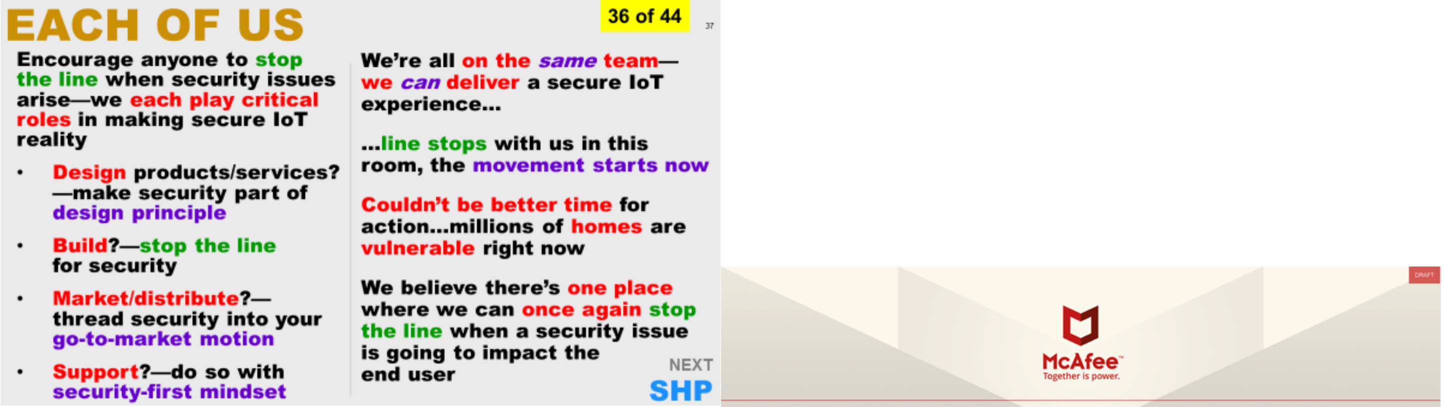
EACH OF US

We need a world – and an IoT experience – where security is inherent in everything we do.

And, if we're being honest with ourselves, our light in securing the IoT today is yellow, at best. We need to get to green. Security cannot continue to be an aftermarket afterthought.

...

SLIDE 36—Ivory McAfee set warmer with red logo, continued



EACH OF US

36 of 44

37

Encourage anyone to stop the line when security issues arise—we each play critical roles in making secure IoT reality

- Design products/services?—make security part of design principle
- Build?—stop the line for security
- Market/distribute?—thread security into your go-to-market motion
- Support?—do so with security-first mindset

We're all on the *same* team—we *can* deliver a secure IoT experience...

...line stops with us in this room, the movement starts now

Couldn't be better time for action...millions of homes are vulnerable right now

We believe there's one place where we can once again stop the line when a security issue is going to impact the end user

NEXT
SHP

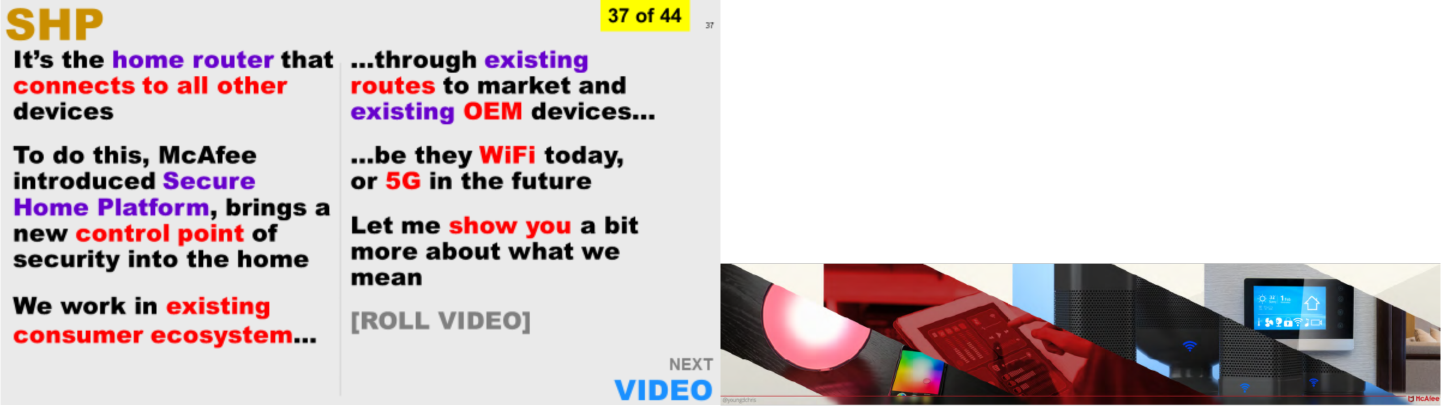
Therefore, our management philosophy must be one that encourages anyone to "stop the line" when security issues arise. Each of us plays a critical role in making a secure IoT world a reality. Do you design products or services? I ask that you consider security as a critical design principle. Do you build products or services? I ask that you build security into the experience. Do you market or distribute for your company? I ask that you thread security into your go-to-market motion. Do you support customers? I ask that you do so with a security-first mindset. We're all on the same team. We all can deliver a secure experience for our customers.

The line stops with those of us in this room and the movement starts now.

And there couldn't be a better case for immediate action. How many households have vulnerable connected devices right now? We believe there is one place in the household where we can once again "stop the line" when a security issue is going to impact the end user.

...

SLIDE 37—Home devices parallelograms



SHP

37 of 44

37

It's the home router that connects to all other devices

To do this, McAfee introduced Secure Home Platform, brings a new control point of security into the home

We work in existing consumer ecosystem...

...through existing routes to market and existing OEM devices...

...be they WiFi today, or 5G in the future

Let me show you a bit more about what we mean

[ROLL VIDEO]

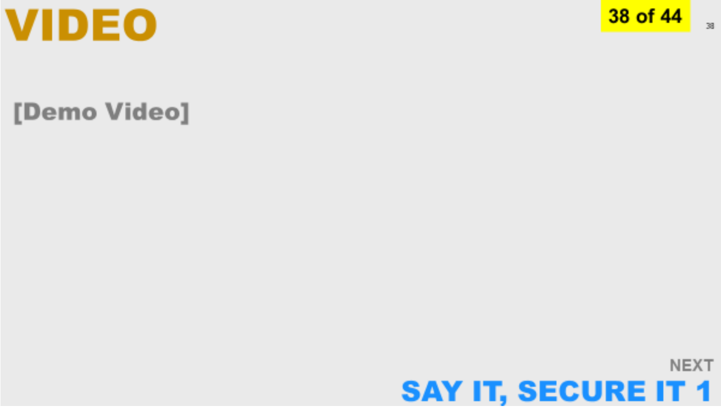
NEXT
VIDEO

It's the home router that connects all devices to it. To do this, McAfee introduced our secure home platform, which brings a new security control point into the home. And, we work within the ecosystem to deliver the secure home platform to the consumer through existing routes to market and existing OEM devices – be they WiFi today or 5G in the future.

Let's show you a bit more about what we mean.

...

SLIDE 38—ALEXA/SHP video, 1:30 (against gray canvas)



VIDEO

38 of 44

38

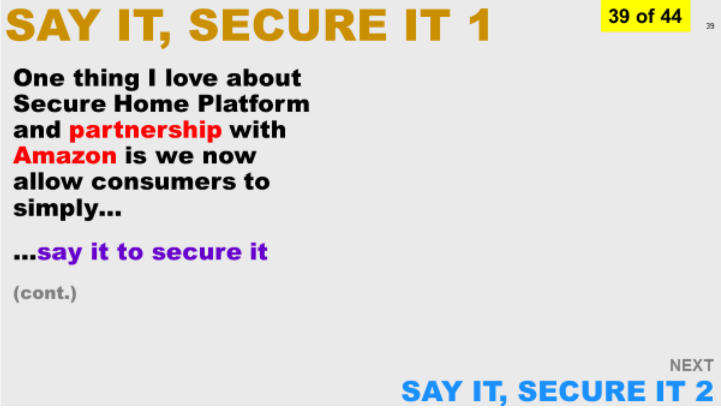
[Demo Video]

NEXT

SAY IT, SECURE IT 1

…

SLIDE 39—Say it to secure it 1



SAY IT, SECURE IT 1

39 of 44

39

One thing I love about Secure Home Platform and partnership with Amazon is we now allow consumers to simply…

…say it to secure it

(cont.)

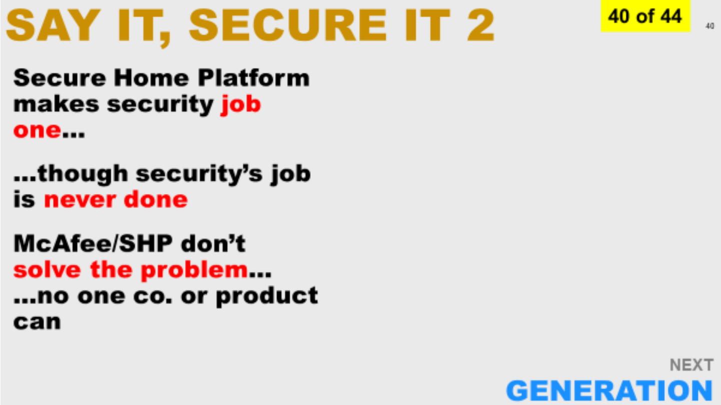
NEXT

SAY IT, SECURE IT 2

One of the things I love about the Secure Home Platform and our partnership with Amazon is that we now allow consumers to simply *say it to secure it.*

…

SLIDE 40—Say it to secure it 2



SAY IT, SECURE IT 2

40 of 44

40

Secure Home Platform makes security job one…

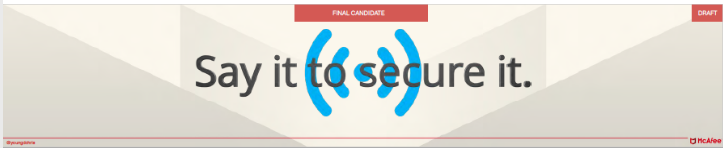
…though security's job is never done

McAfee/SHP don't solve the problem…

…no one co. or product can

NEXT

GENERATION

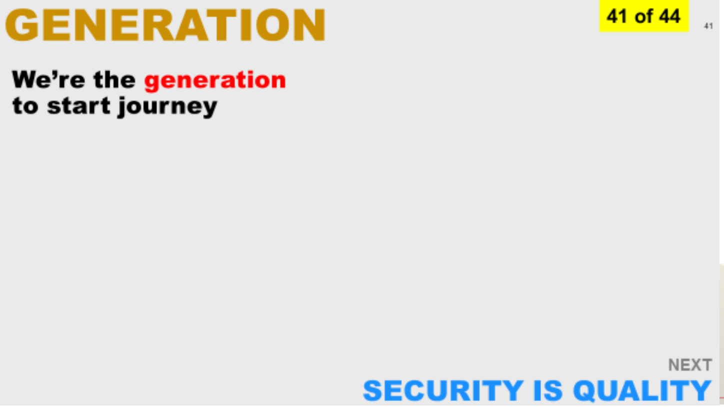


The secure home platform makes security job one, though security's job is never done.

Neither McAfee, nor our secure home platform, solves for the entire problem – no one company or product can.

…

SLIDE 41—Logo



GENERATION

41 of 44

We're the generation to start journey

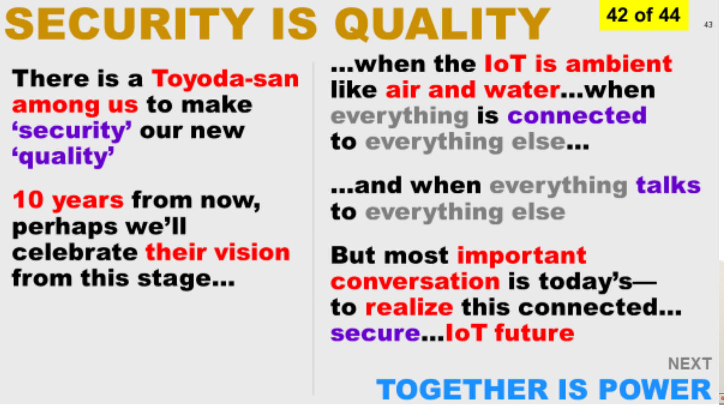
NEXT

SECURITY IS QUALITY

But we are the generation that will start us on this journey.

…

SLIDE 42—Cybersecurity is quality.



SECURITY IS QUALITY

42 of 44

There is a Toyoda-san among us to make 'security' our new 'quality'

10 years from now, perhaps we'll celebrate their vision from this stage…

…when the IoT is ambient like air and water…when everything is connected to everything else…

…and when everything talks to everything else

But most important conversation is today's—to realize this connected… secure…IoT future

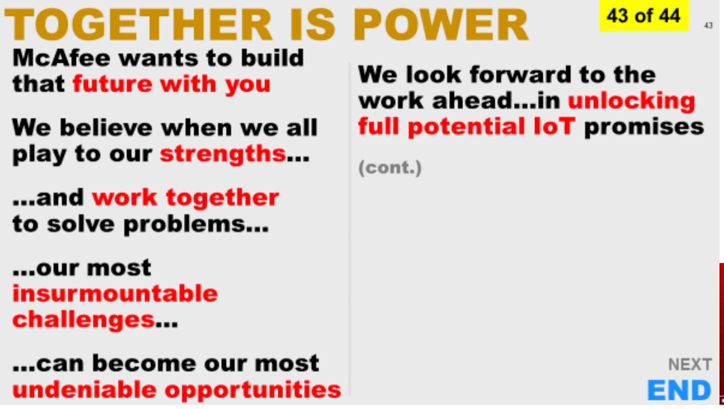
NEXT

TOGETHER IS POWER

There is a Toyoda-san among us who will make "security" the "quality" of our time. And, ten years from now, perhaps someone from this keynote stage will admire that person, when the IoT is as ambient as air and water. When everything is connected to everything else. When everything talks to everything else. But, the most important conversation is the one we are having today to realize this connected, secure IoT future.

…

SLIDE 43—Red McAfee set warmer with white logo



TOGETHER IS POWER

43 of 44

McAfee wants to build that future with you

We believe when we all play to our strengths…

…and work together to solve problems…

…our most insurmountable challenges…

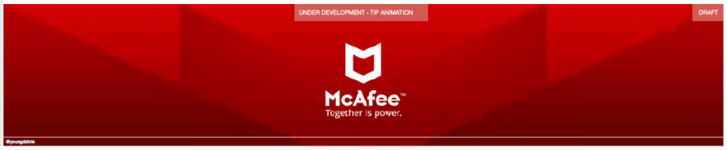
…can become our most undeniable opportunities

We look forward to the work ahead…in unlocking full potential IoT promises

(cont.)

NEXT

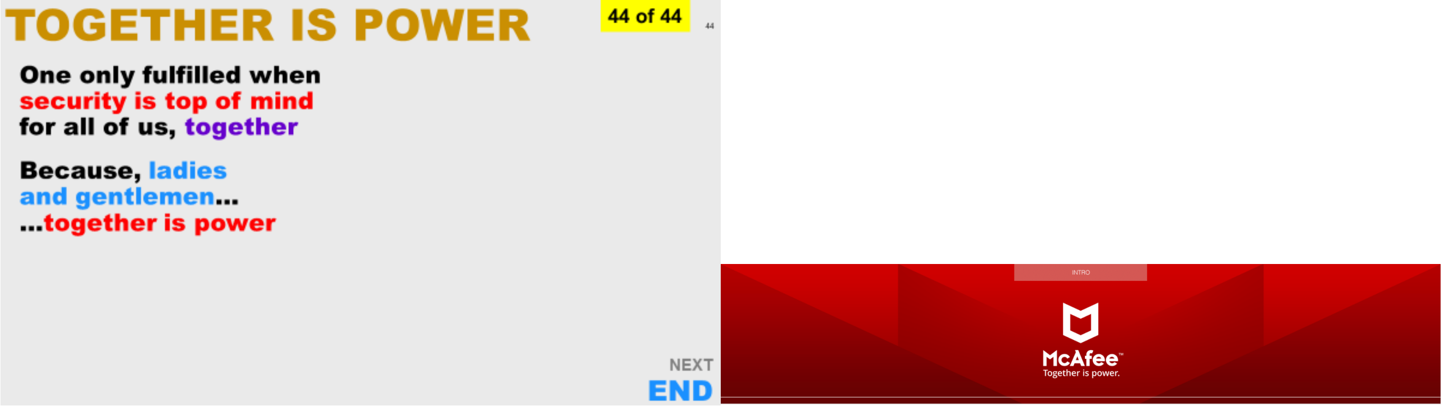
END



We at McAfee want to build that future with you. We believe that, when we all play to our strengths and work together to solve problems, the most insurmountable challenges become the most undeniable opportunities. We look forward to the work ahead in unlocking the full potential the IoT promises…

…

SLIDE 44—Together is Power animation



TOGETHER IS POWER

44 of 44

44

One only fulfilled when
security is top of mind
for all of us, together

Because, ladies
and gentlemen…
…together is power

NEXT
END

…one that can only be fulfilled when security is top of mind for all of us, together. Because, ladies and gentlemen, together is power.

<END>