FORTINET®

2012 IT Security Survey

June 2012 - Fortinet

Methodology

- Survey company: Vision Critical (Independent third party – UK based)

- Respondents:
  - Worldwide survey conducted in 15 territories during May/June 2012
  - 3,800+ active employees in full time employment aged 20 to 29
  - University graduate level individuals
  - Owners of personal smartphone, tablet or laptop

Agenda

1 BYOD is here to stay

2 Security challenges posed by BYOD

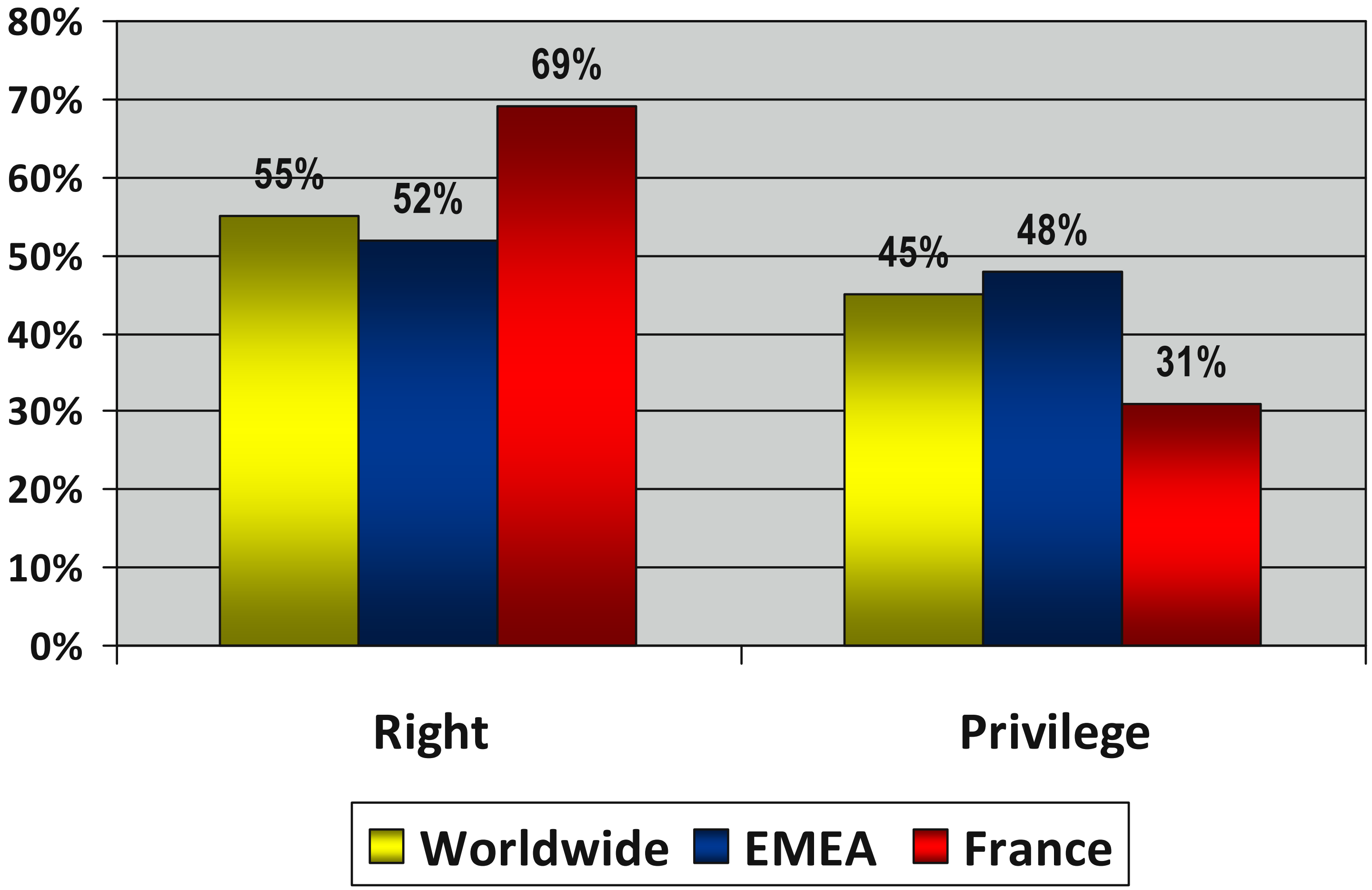
3 Fortinet proposition towards BYOD

How often do Gen-Y workers use their personal devices for work purposes?

	Worldwide	*EMEA*	*APAC*	*US*	*France*
Never	8%	9%	4%	14%	12%
Very occasionally – a few times a year	10%	10%	6%	15%	15%
Every so often – once or twice a month	7%	8%	5%	10%	8%
Regularly – a few times a month	10%	10%	8%	12%	8%
Most days	20%	21%	21%	17%	12%
Every day	45%	42%	56%	33%	45%
BYOD Workers	**74%**	**73%**	**85%**	**61%**	**64%**

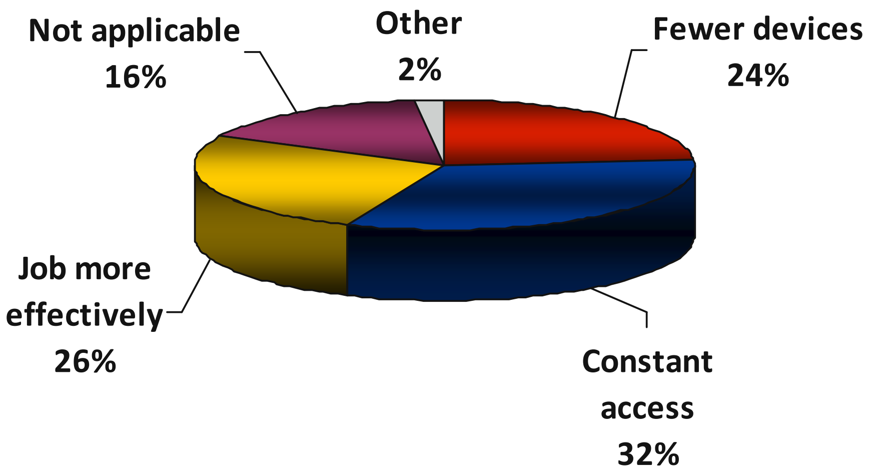
74% of respondents accross all territories compared to 64% in France already regularly engaging in the BYOD practice

Which statement best sums up the attitude of Gen-Y workers to using their own personal device for/at work ?

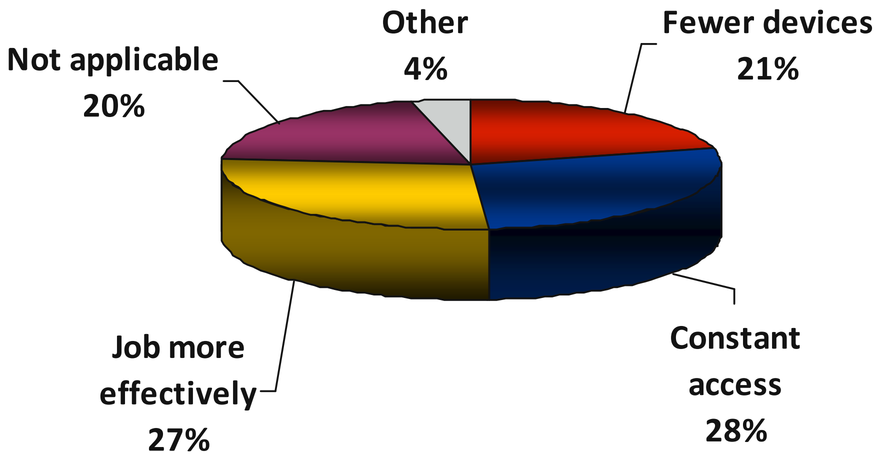


What is the main reason for Gen-Y workers to use their own device for work purposes?

Worldwide

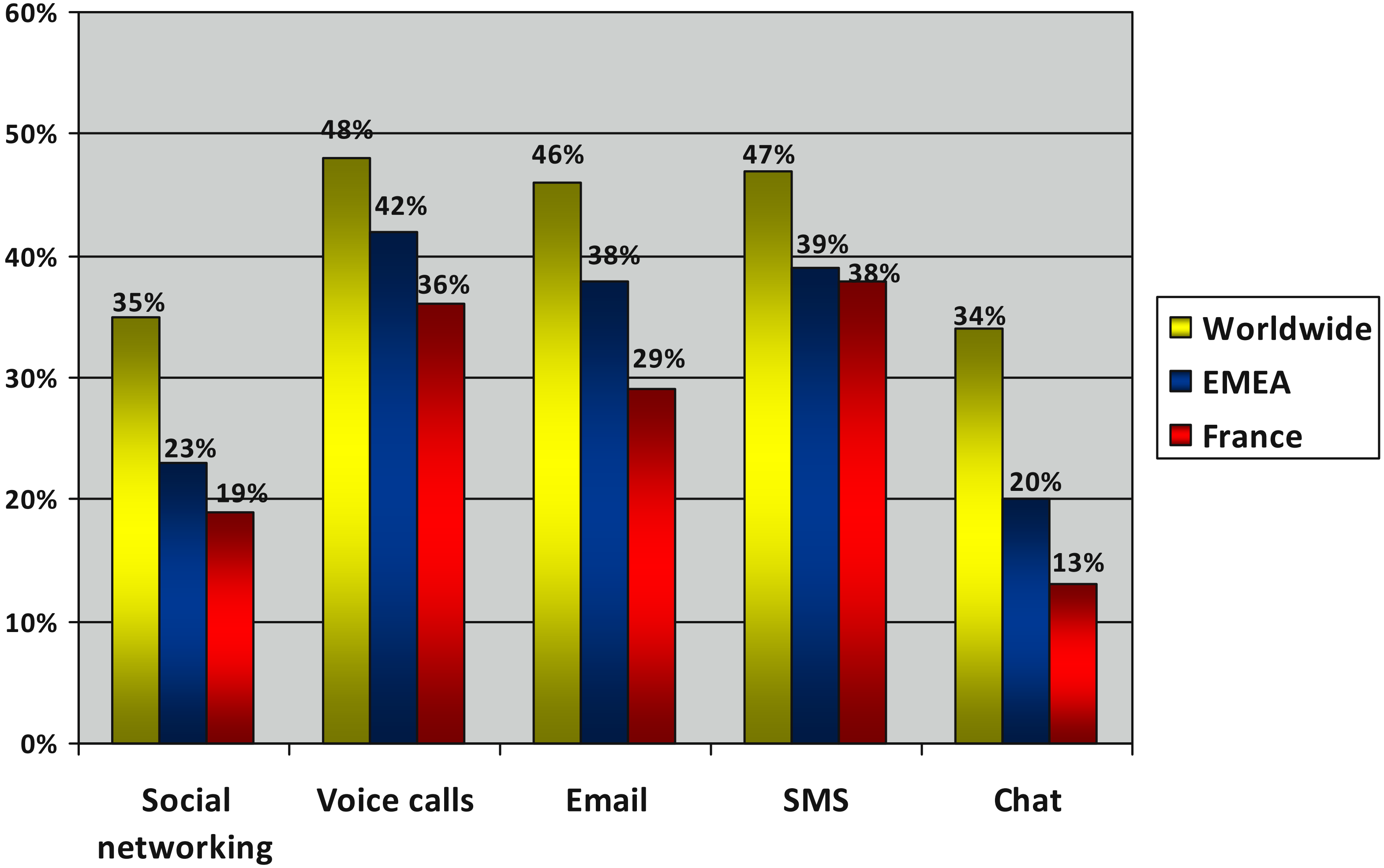


France



26% of all respondents (27% in France) said it allows them to do their job more effectively

What are the situations Gen-Y workers couldn't live without for more than a day?



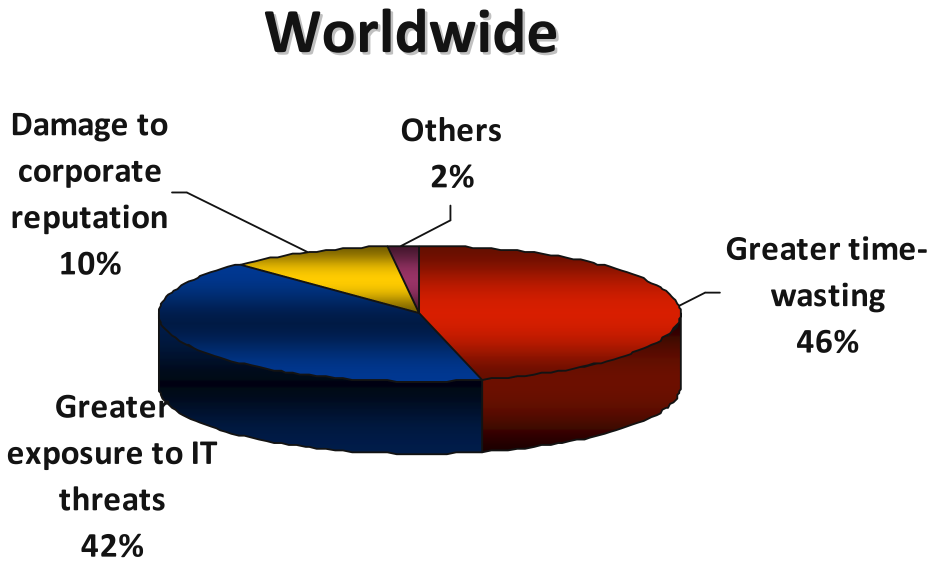
Agenda

1 BYOD is here to stay

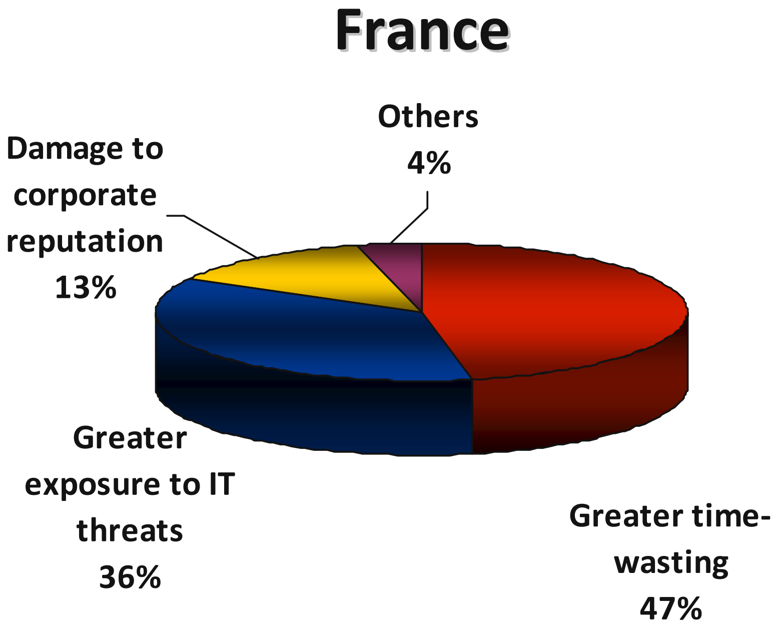
2 Security challenges posed by BYOD

3 Fortinet proposition towards BYOD

What is the greatest risk posed by BYOD to the organization?



46% cited lost productivity and 42% cited exposure to malware



In France, 47% cited lost productivity and 36% cited exposure to malware

Have Gen-Y workers ever/would use a personal device in contravention of the corporate policy?

Personal devices

	Worldwide	*EMEA*	*APAC*	*US*	*France*
Yes	36%	27%	47%	29%	30%
No	64%	73%	53%	71%	70%

Non-approved applications

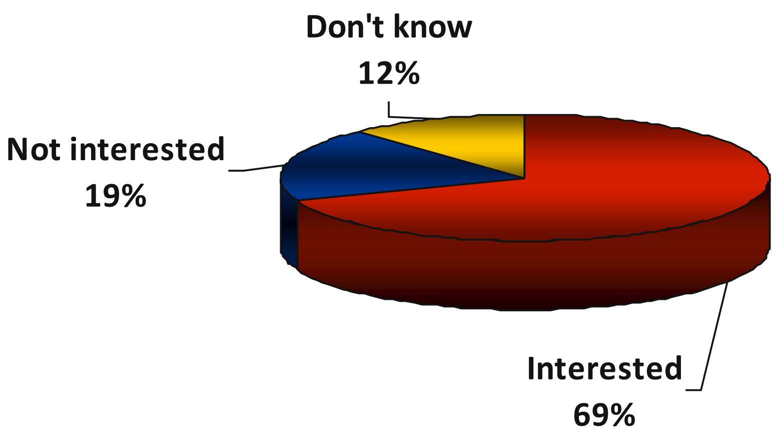
	Worldwide	*EMEA*	*APAC*	*US*	*France*
Yes	30%	22%	39%	26%	25%
No	70%	78%	61%	74%	75%

1-in-3 all people (30% in France) would contravene company policy banning the use of personal device for work purposes

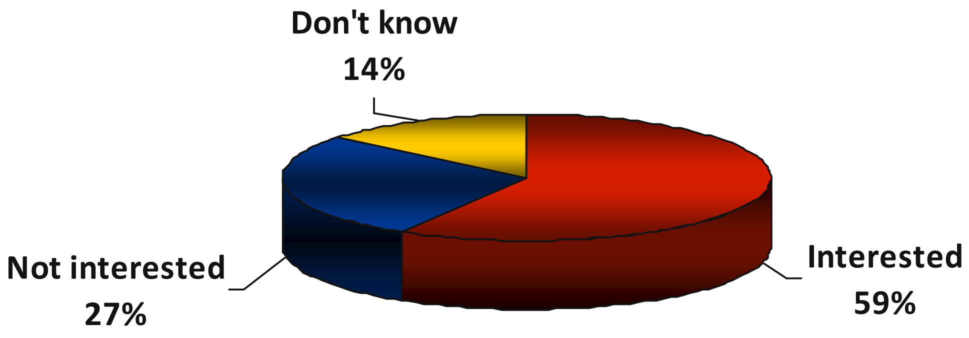
30% of all respondents (1-in-4 in France) would contravene company policy banning the use of app for work purposes

If creating their own applications for work was quick & easy – how likely would Gen-Y workers do it?

Worldwide



France



	Worldwide	EMEA	APAC	US	France
Very likely	29%	29%	34%	20%	23%
Quite likely	40%	40%	47%	32%	35%
Quite unlikely	10%	8%	10%	12%	12%
Very unlikely	9%	11%	3%	14%	15%
Don’t Know	12%	12%	6%	22%	14%

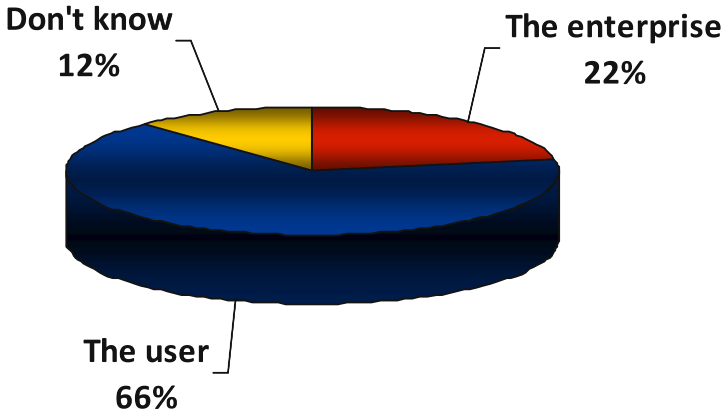
What repercussions would make Gen-Y workers more vigilant when using their personal devices for work?

	Worldwide	EMEA	APAC	US	France
Putting the public reputation of your employer at risk	21%	24%	20%	18%	19%
Being prevented from accessing personal applications while at work	33%	26%	43%	25%	28%
Being prevented from using your personal device of choice, for work	16%	14%	18%	16%	14%
Being subject to employer disciplinary action	21%	24%	13%	30%	26%
Poorer future employment prospects	9%	12%	6%	10%	11%
Other, please specify	1%	1%	0%	2%	2%

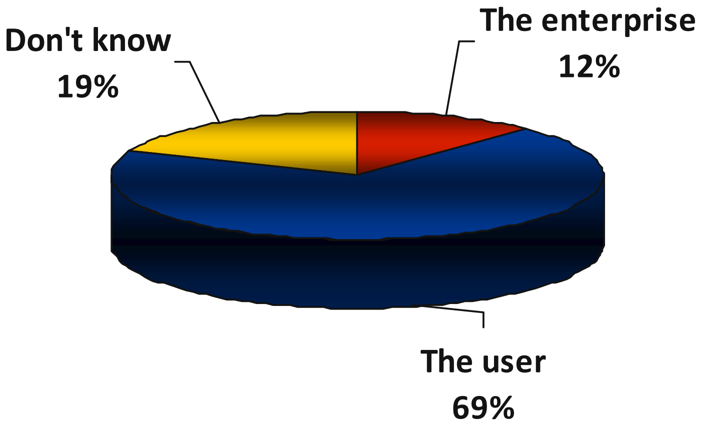
The risk of being denied access to personal app was the main concern for respondents

Who is responsible for the security of personal device when used for work purposes?

Worldwide



France



	Worldwide	*EMEA*	*APAC*	*US*	*France*
The organisation is ultimately responsible	22%	14%	36%	12%	12%
I am ultimately responsible	66%	74%	53%	74%	69%
Don’t know	12%	12%	11%	14%	19%

Agenda

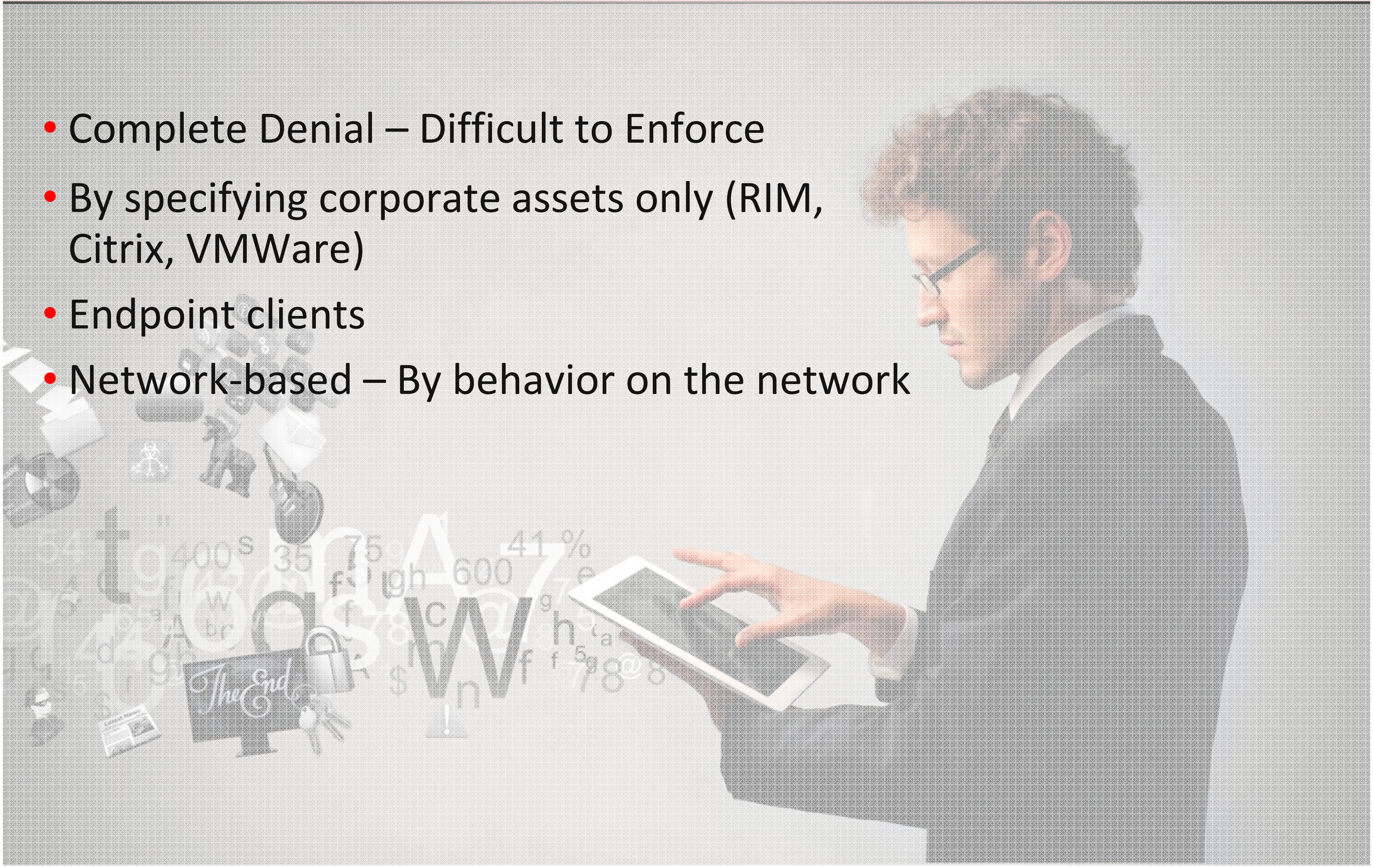
1 BYOD is here to stay

2 Security challenges posed by BYOD

3 Fortinet proposition towards BYOD

BYOD Management: Through Corporate Policy

- Complete Denial – Difficult to Enforce
- By specifying corporate assets only (RIM, Citrix, VMWare)
- Endpoint clients
- Network-based – By behavior on the network



Fortinet Lets Organizations Say Yes To BYOD

APPS

Controlling Apps & Features Within Apps

- Categories of Apps
- Individual Apps
- Actions Within Apps

USERS

Defining User Behavior

- By Domain
- By Groups
- By Individual Users

DATA

Controlling Data

- Prioritize
- Limit Access By Groups or Users
  - Time of Day
  - Day of Week

Protecting All BYOD Attack Vectors

Email Sent – Contains Sensitive Data

Mail message detected as Data Loss (DLP)

User accesses phishing site, enters credentials

Access to phishing website is blocked

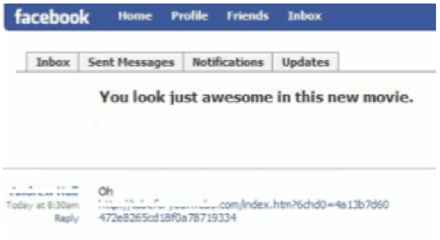
Phishing site sends Bot infection to user disguised as 'Security Update' application

Content scanning prevents download

End user executes BOT application, is infected and now all their data is compromised

Botnet command channel is blocked, no compromised data can be sent

Secure BYOD In Action



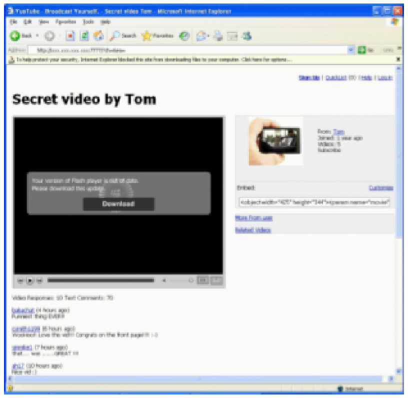
You look just awesome in this new movie.

Today at 8:30am
Reply

Oh
…com/index.htm?6chd0=4a13b7d60 472e8265cd18f0a78719334

“Innocent” Video Link:

»Redirects to malicious Website


YouTube - Broadcast Yourself. - Secret video Tom - Microsoft Internet Explorer
Download
Embed
Customize
More From user
Related Videos

Secret video by Tom

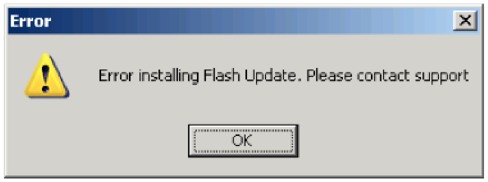
Your version of Flash player is out of date.
Please download this update.

From: Tom
Joined: 1 year ago
Videos: 5
Subscribe

Video Responses: 10 Text Comments: 70

“Out of date” Flash player

»Download malware file



Error installing Flash Update. Please contact support

Error message:

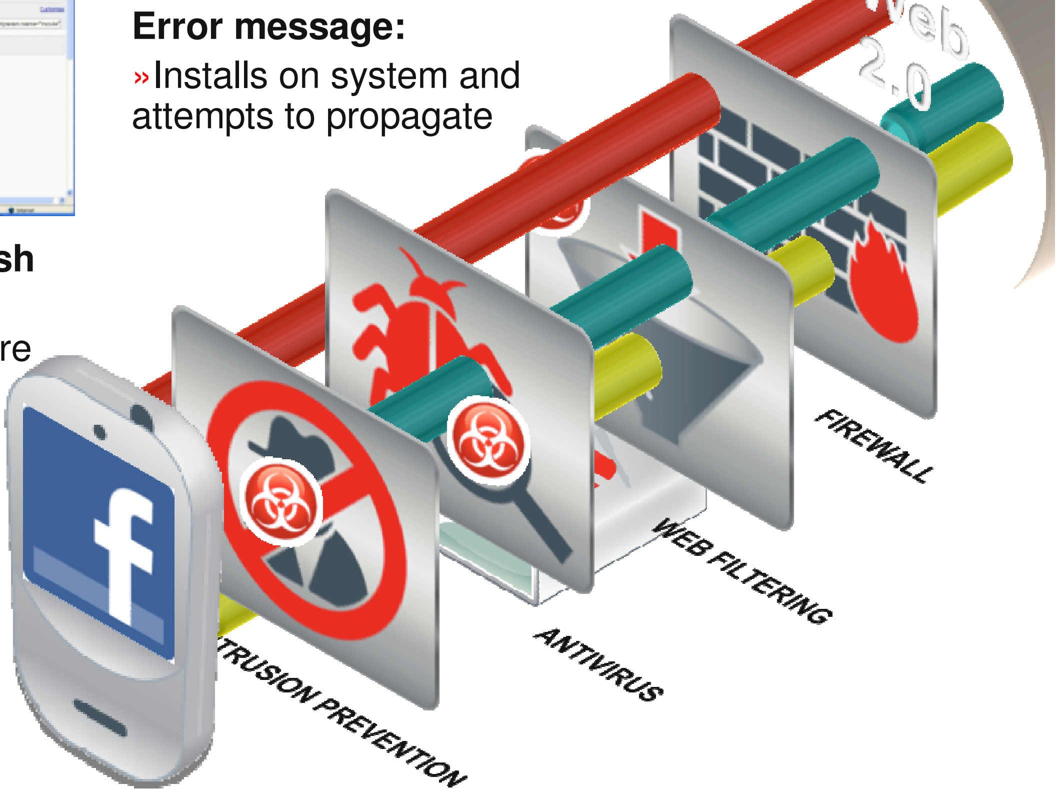
»Installs on system and attempts to propagate

Integrated Web Filtering
Blocks access to malicious Website

Network Antivirus
Blocks download of virus

Intrusion Prevention
Blocks the spread of the worm

Authentication & Encryption



THANK YOU