

The A Register[®]

Security: knowing what
you don't know

And what you can do about it



Why are we here?

100 per cent security is a fantasy.

How do you cope with reality?

On our Regcast today

Raimund Genes, **Trend Micro**

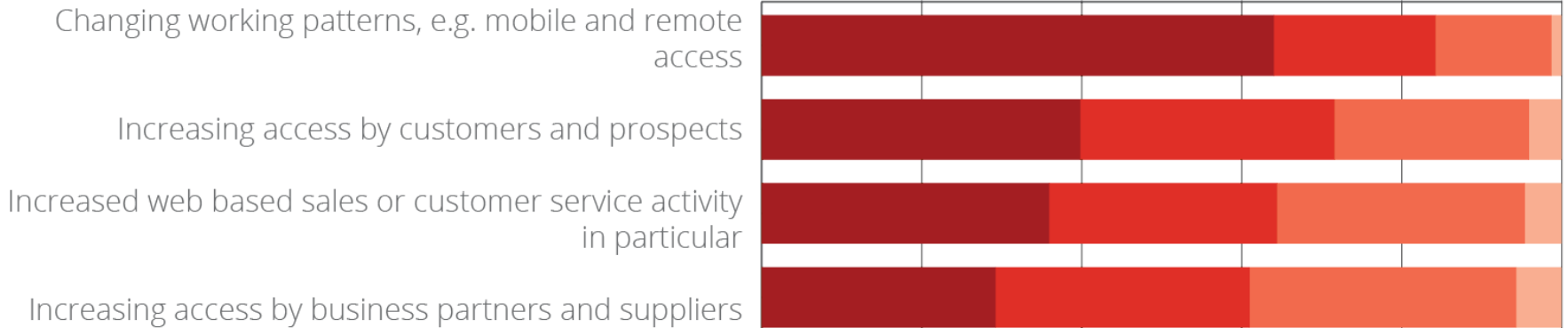
Tony “Dark Lord” Lock, **Freeform Dynamics**

Tim Phillips, **The Reg**

Do these things make application access security harder?

APPLICATION ACCESS VIEW

0% 20% 40% 60% 80% 100%



SYSTEMS AND DATA VIEW



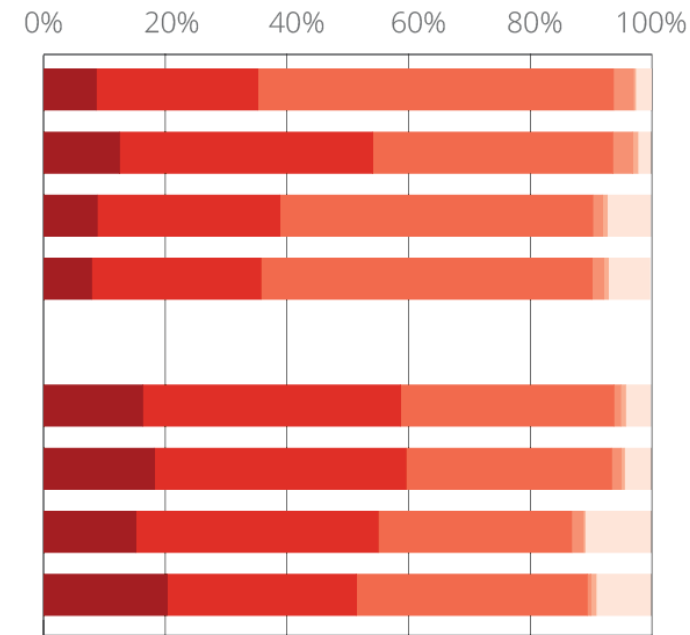
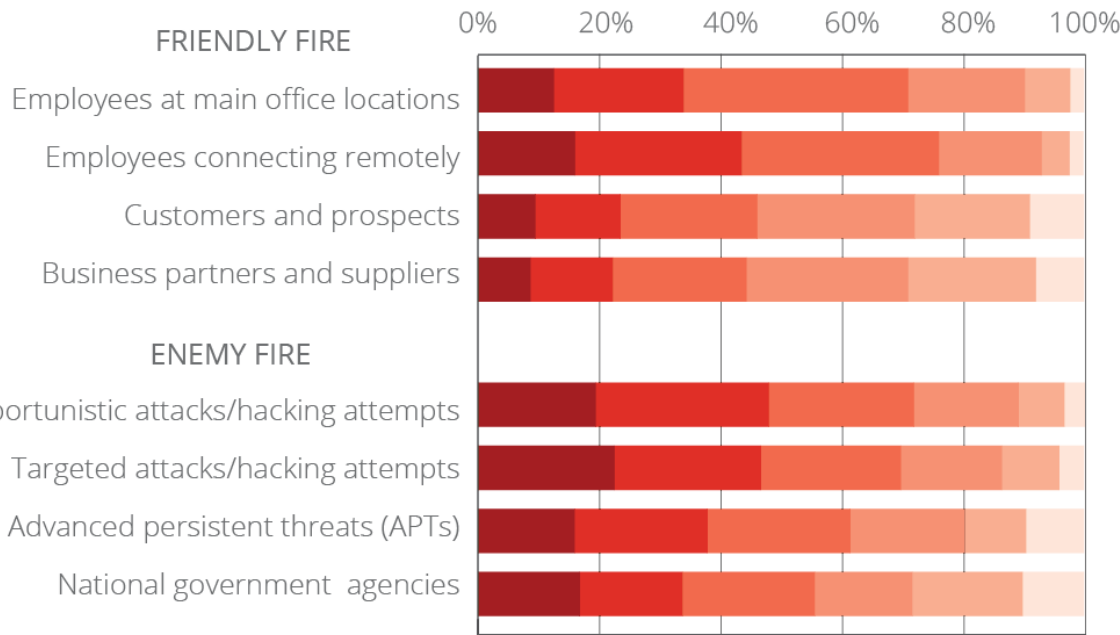
Yes
 No, but likely to in the future
 No and unlikely to
 Unsure

How much of a perceived security threat (including ignorance or mishap) are...?

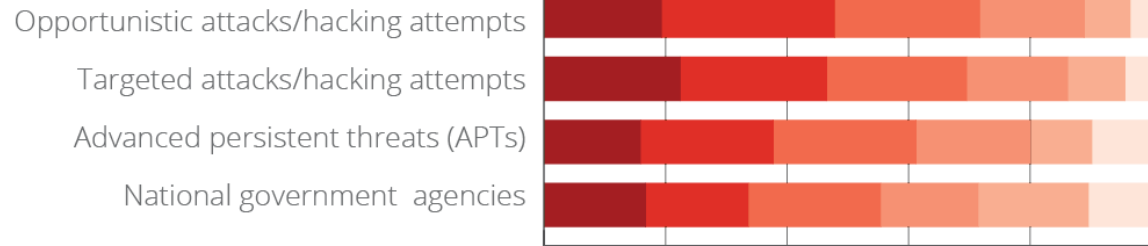
PERCEIVED THREAT NOW

PERCEIVED THREAT 3 YRS TIME

FRIENDLY FIRE



ENEMY FIRE





SCRIPT KIDDIES

Nothing says amateur like having only an "anonymous" proxy server between you and a Vice Presidential candidate and federal law enforcement

by cybertalk.com



How to get your prey

Probing

Compromising

Stealing

**Research -
Target a victim**



**Social Engineering
- get them to click**



**Own one machine
inside perimeter**



**Probe internal
network**

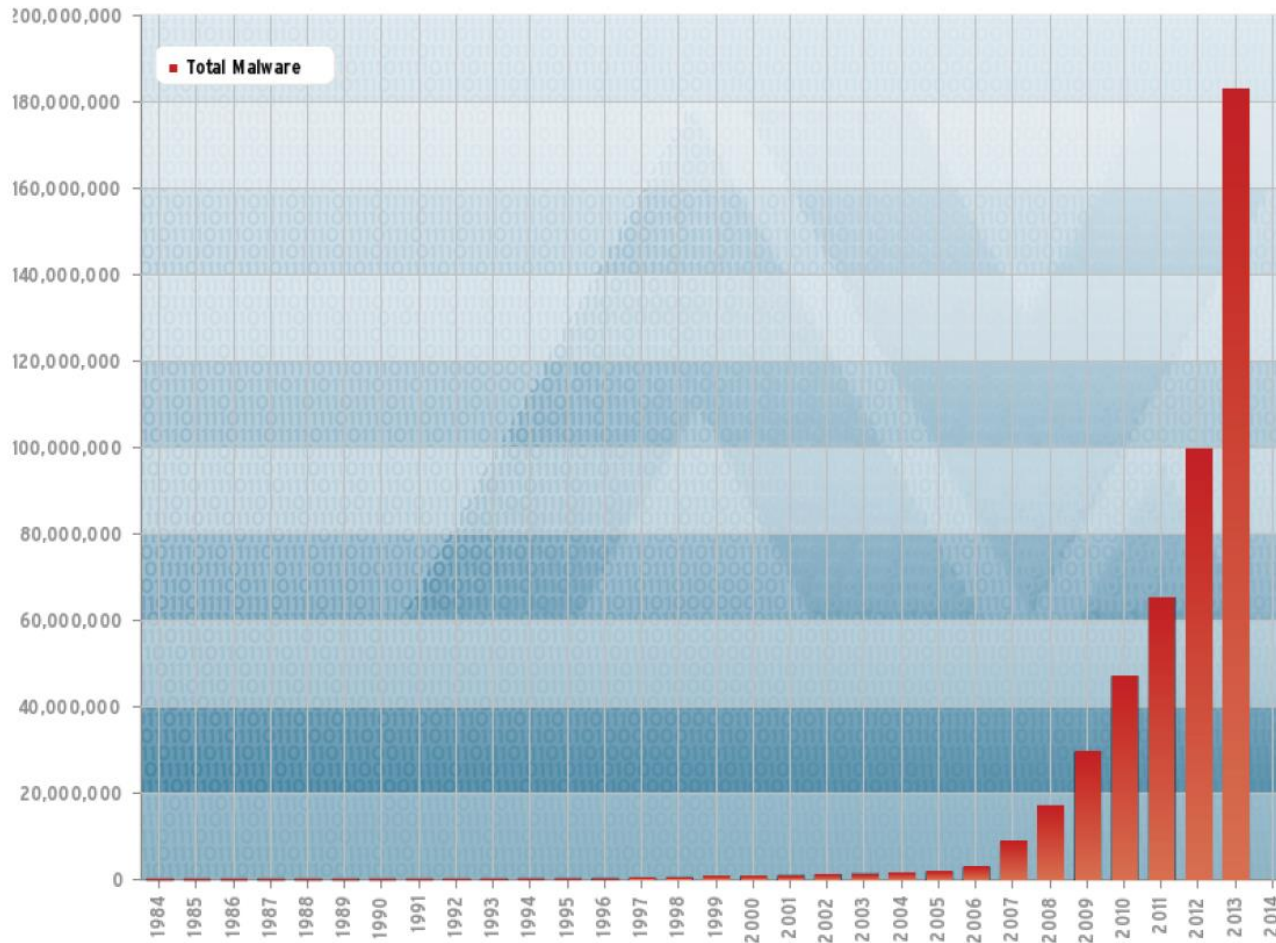


**Compromise key
servers**



Steal your data

AV-Test malware stats



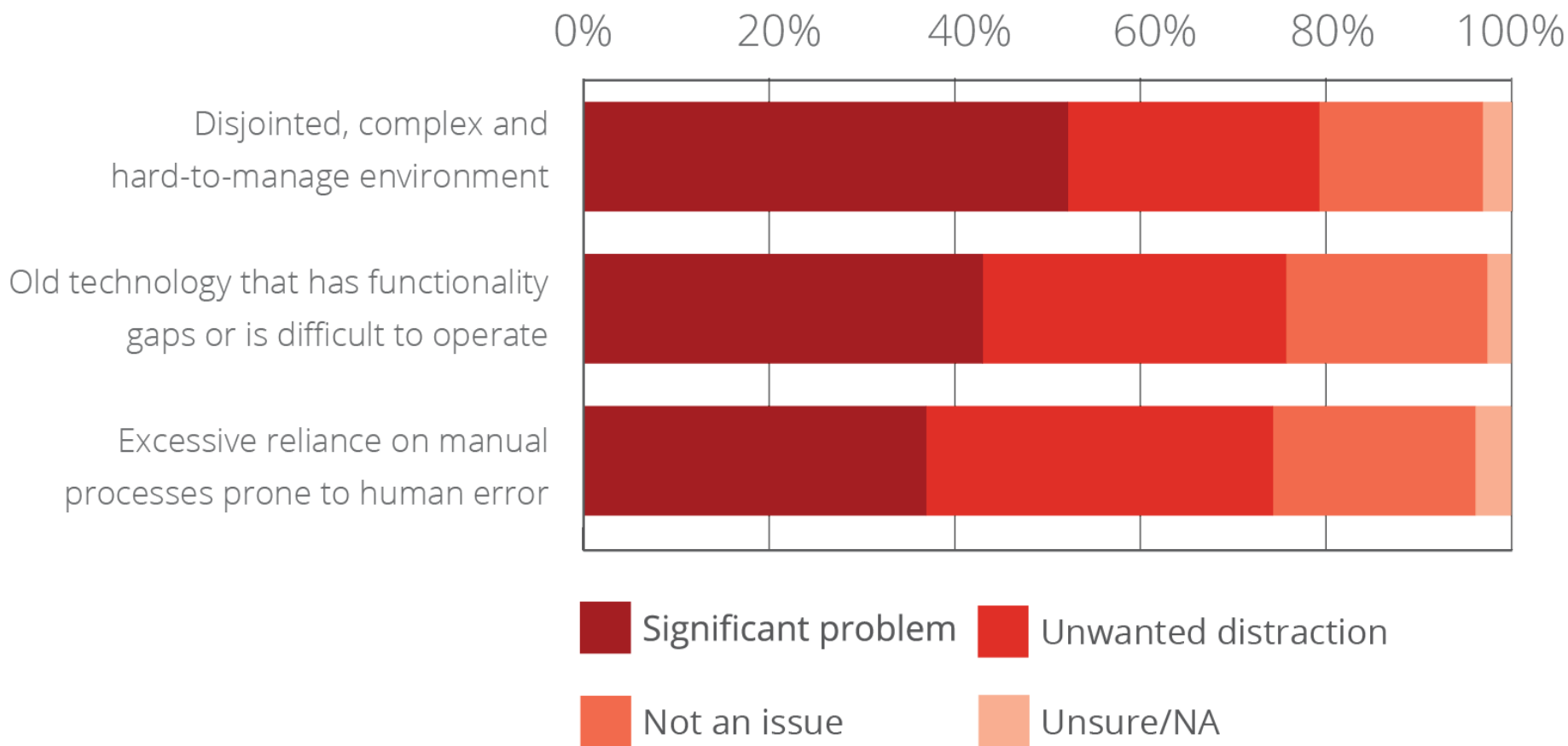
Last update: 01-02-2014 14:11

Copyright © AV-TEST GmbH, www.av-test.org

People who want to get in, get in



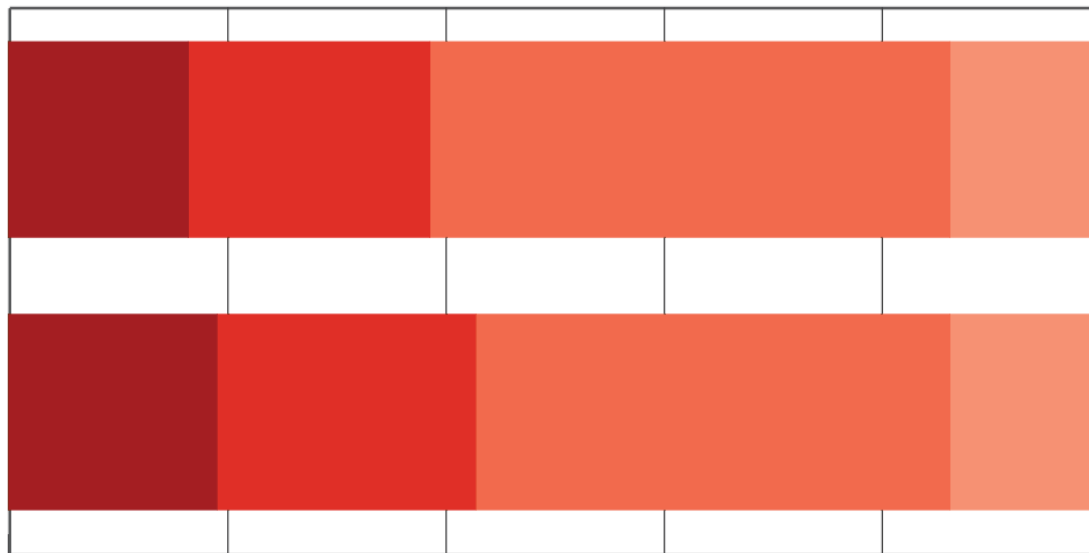
Managing application performance, availability and security problems



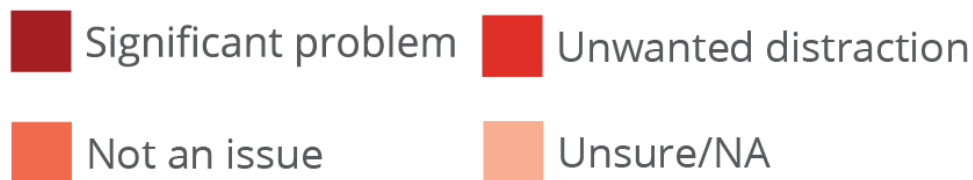
Managing application performance, availability and security problems

0% 20% 40% 60% 80% 100%

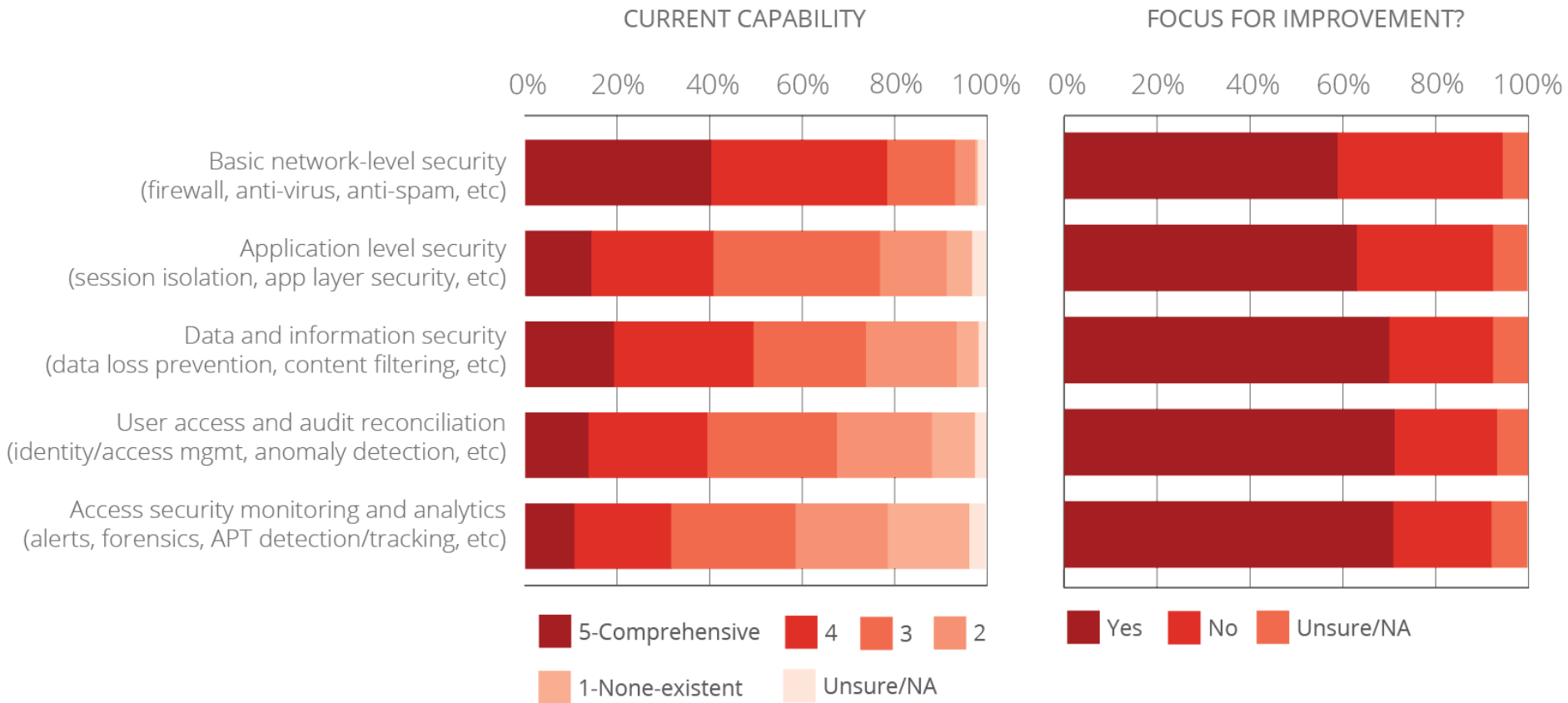
Hard to manage cloud and on-premise service levels in a coherent manner



Hard to manage cloud and on-premise security in a coherent manner

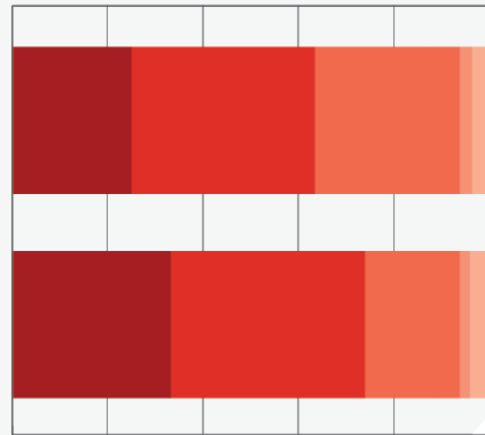


Your access security capability



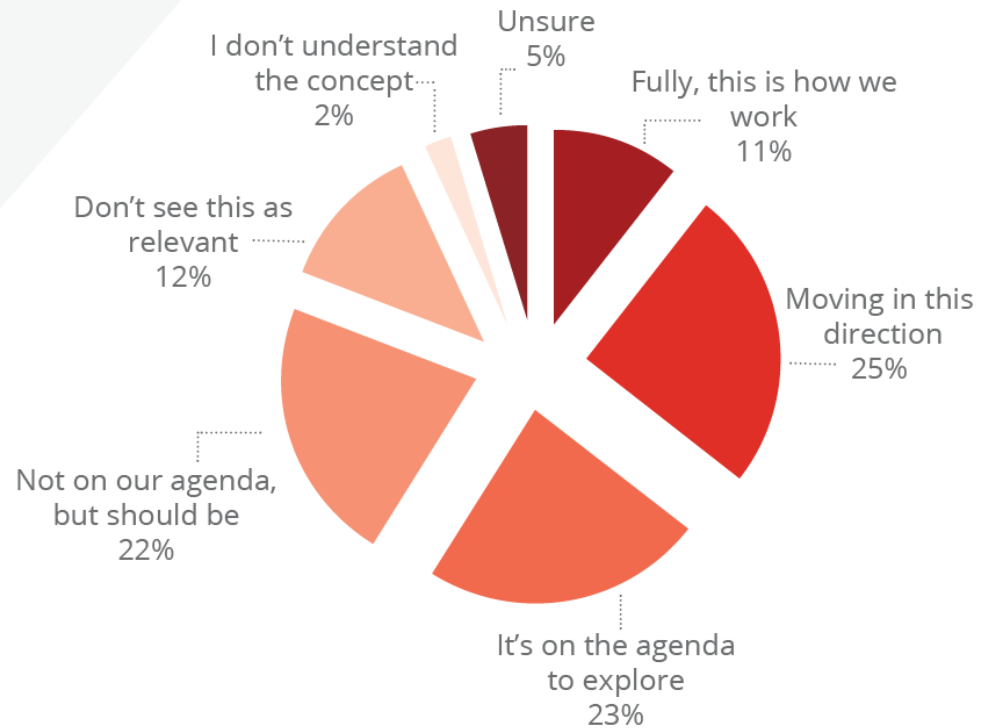
How secure is your data?

0% 20% 40% 60% 80% 100%



■ Strongly Agree ■ Agree
■ Disagree ■ Strongly Disagree
■ Neutral ■ Unsure/NA

Have you moved from the 'network perimeter' to the 'application perimeter' approach?



The new reality



Information no longer protected by traditional defences



Point solutions; limited visibility, decentralised administration



Dynamic, complex environment; many new apps and platforms



What users need

Smart protection for information



Simple yet flexible to manage and deploy



Security that fits an evolving ecosystem

A complete lifecycle

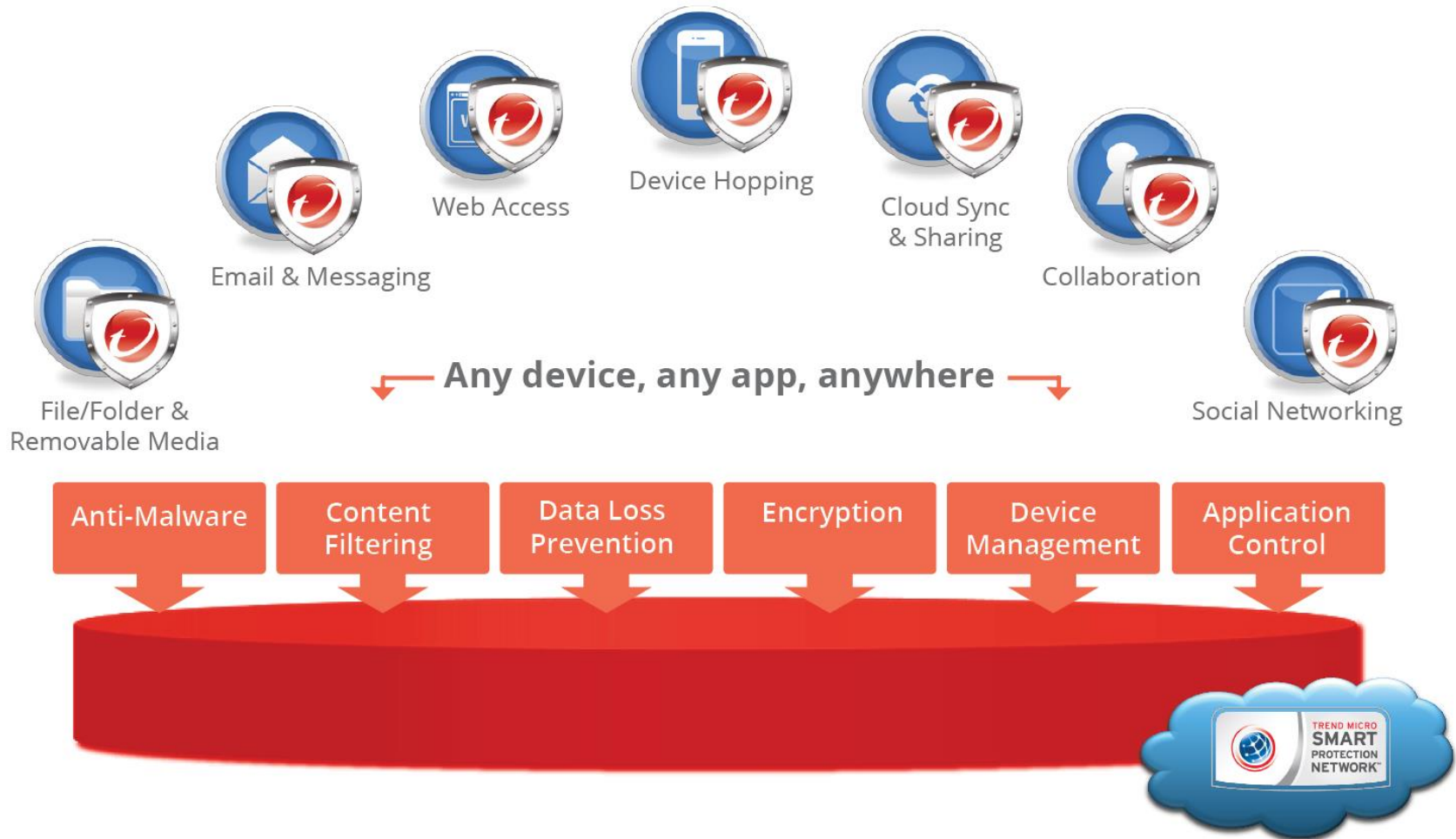
Detect malware, communications and behaviour invisible to standard defences

Analyse the risk and characteristics of the attack and attacker

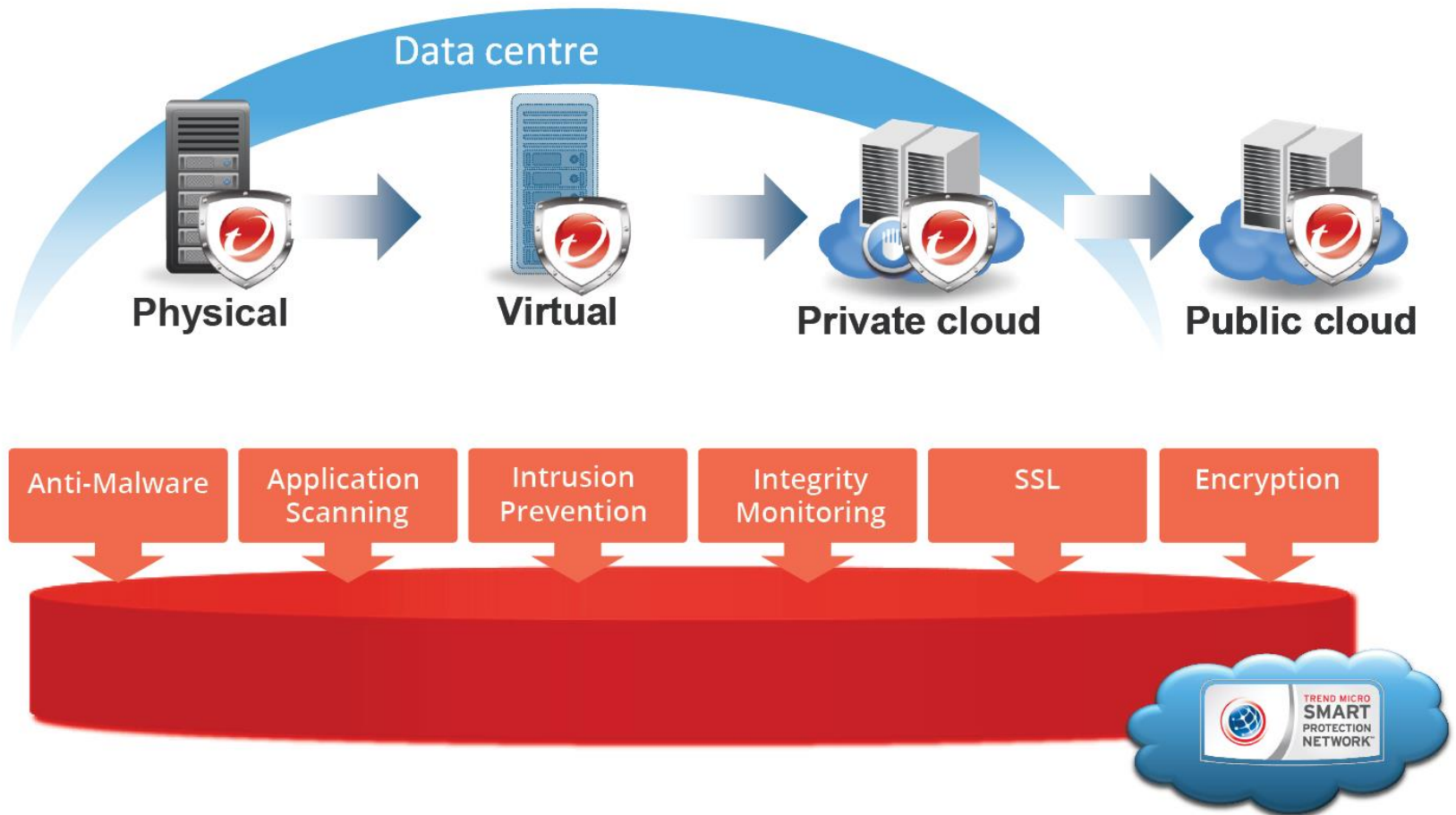
Adapt security automatically (IP blacklists, custom signatures...)

Respond using the insight needed to respond to your specific attackers

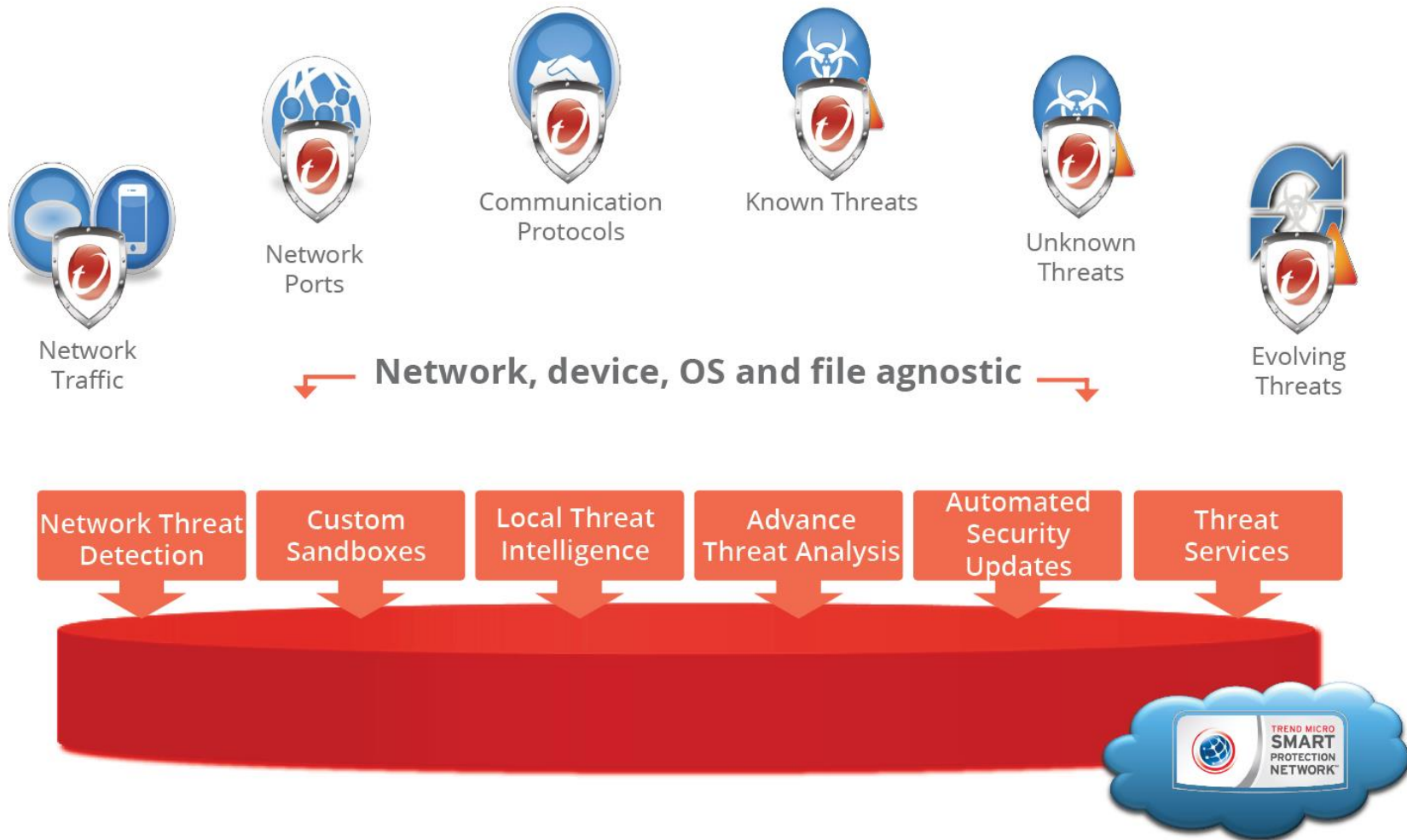
Complete user protection



Cloud and data centre security



Custom defence



Smart protection

Informed know where your data resides

Layered protection from mobile to cloud...from OS to application

Interconnected security across layers, with greater context

Real-time global threat intelligence with faster protection

Transparent enforcement with minimal user impact

Best practice

1. Data breach protection

A layered security model that gives you improved situational awareness across your environment.

2. Privacy

Vendors share what data they obtain and where your data is stored. Encryption is key.

3. Vulnerabilities

Look to virtual patching for non-supported OS and apps.

4. IoE

If developing, build security into framework; if using, build security into the framework.

Further reading

Trend Micro
2014 Threat Predictions: <http://reg.cx/2abg>

Trend Micro
2013 Security Round Up: <http://reg.cx/2abh>

Freeform Dynamics
Controlling Application Access: <http://reg.cx/2ac6>

Thanks for joining us



An archived version of today's event will be made available on The Register in the near future.
