RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

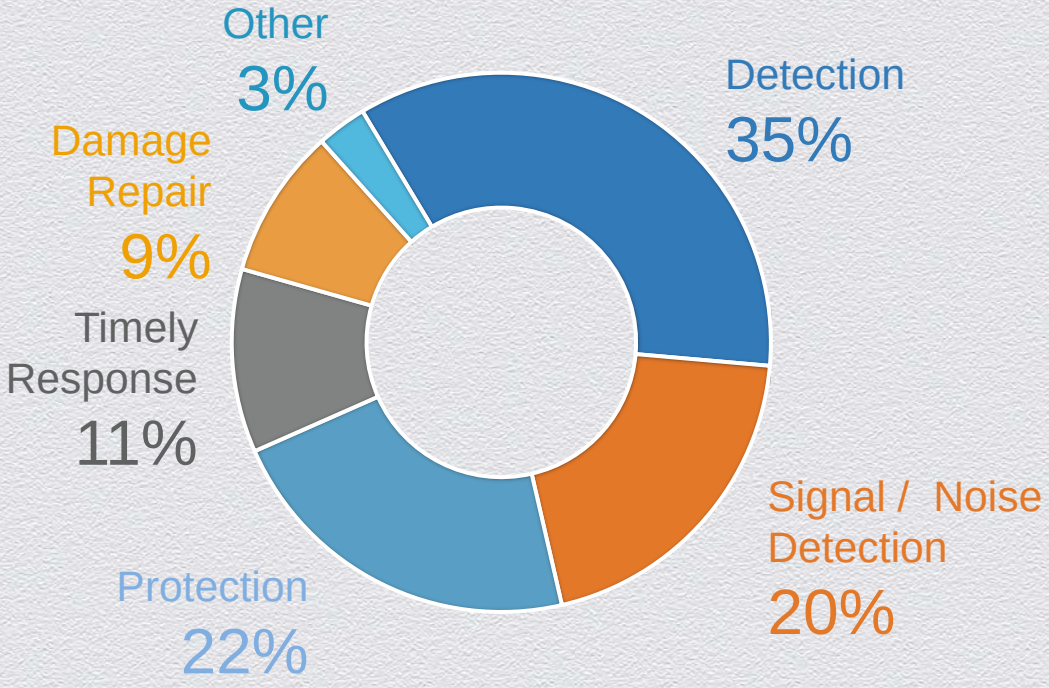
One Step Ahead Of Advanced Attacks and Malware

SESSION ID: SPO2-W02

Jon Paterson

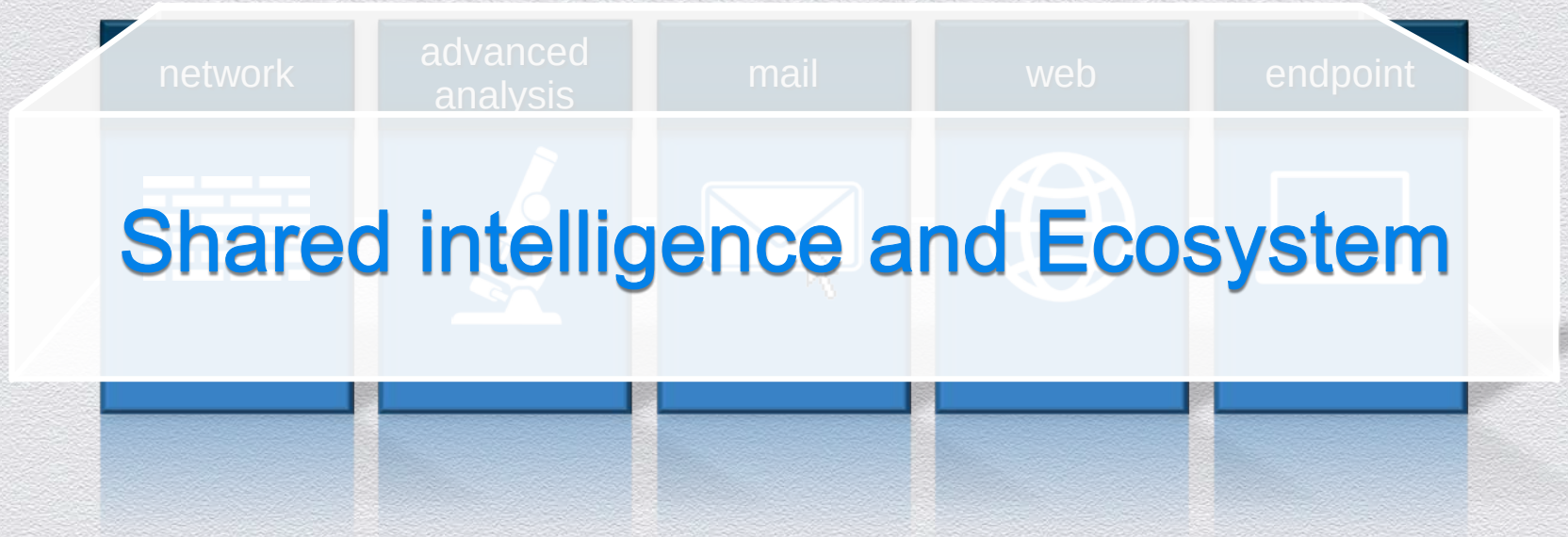
Director, Advanced Technology Group
McAfee, an Intel Company

Advanced malware - what are your concerns?



Source: McAfee Survey at Black Hat USA 2013

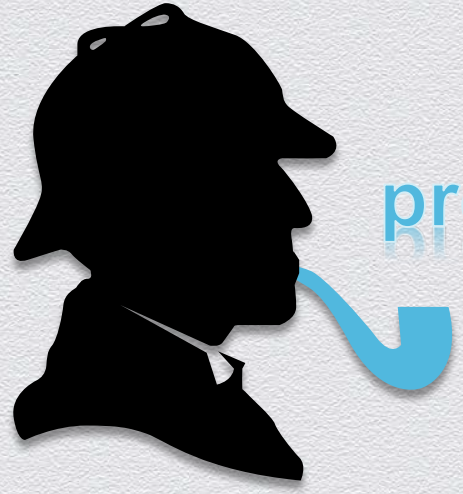
Areas of innovation



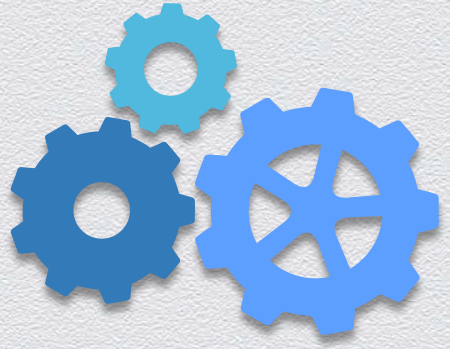
endpoint

next generation Endpoint

how does it Work?



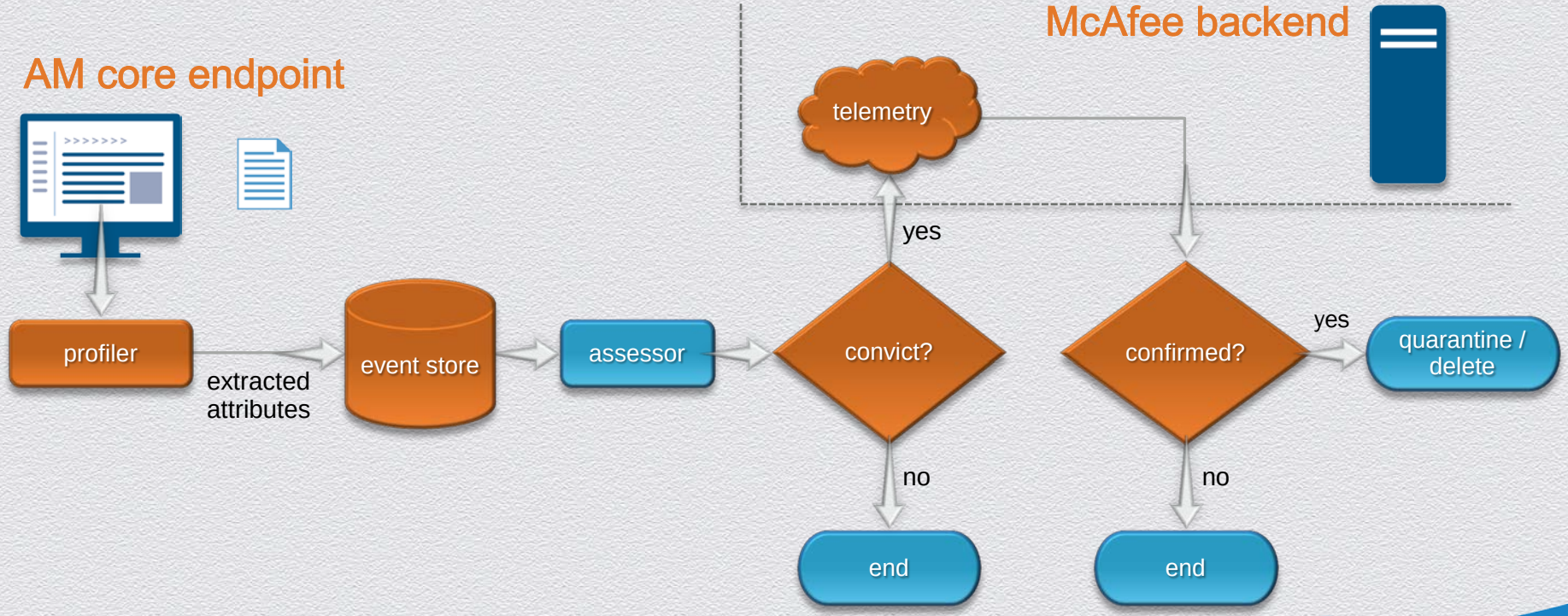
profiler



machine learning

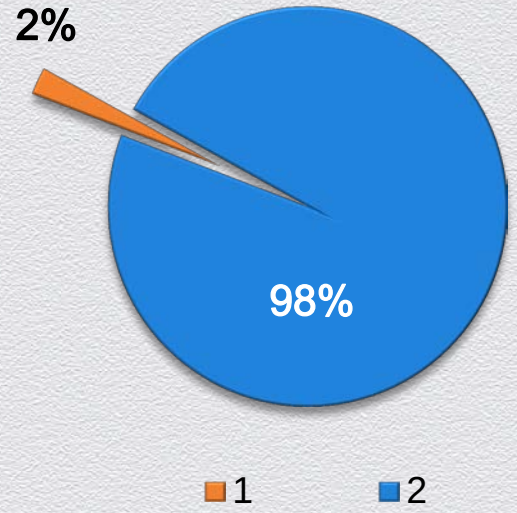
assessor

conviction flow via Assessor



“profiler.gen.a” in Action

- 9360 unique detections
- at moment of detection:
  - 208 previously detected and classified by McAfee
  - 9152 proactive (98%)
- Multiple Family classifications
  - Zbot (24 variants), ZeroAccess (6 variants), FakeAlert (6 variants), WinWebsec,Swisyn,vundu

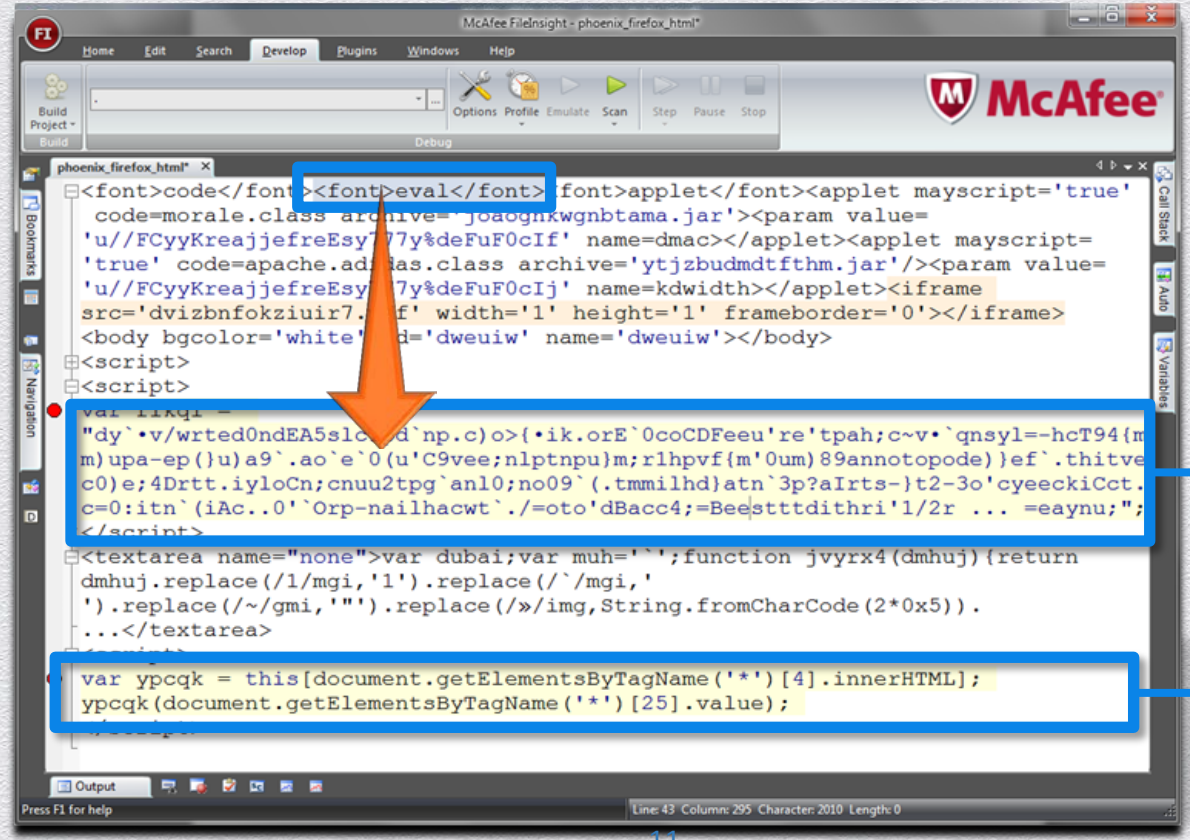


web

Web Exploitation continues as key vector

Images courtesy of kahusecurity.com

Browser DOM specific behavior



exception handling as anti-emulation technique

"eval()" reconstructed

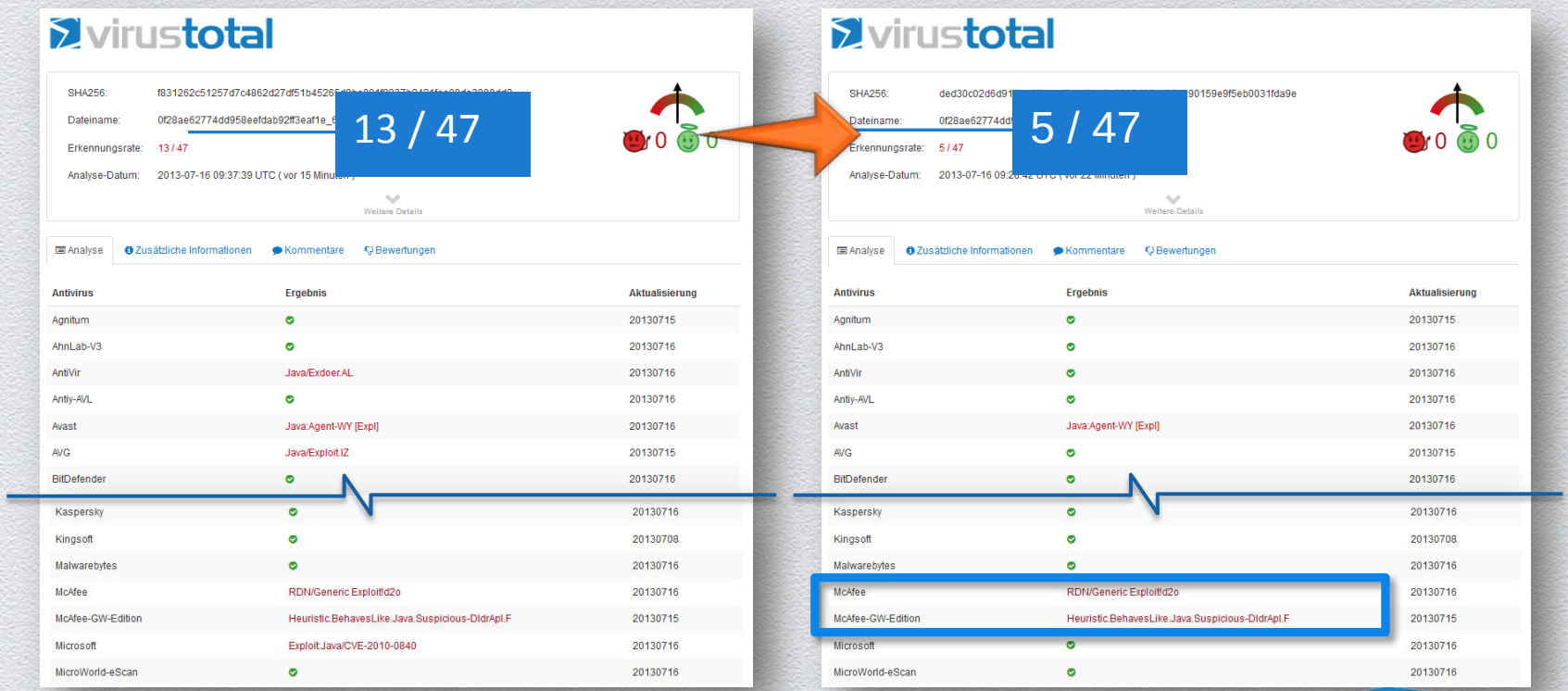
Server side polymorphism

```
{
  Glocker glocker = getGL("setSec" + "urity" + "Man" + "ager", new Object[1]);
  String udfhdk = "rfbc35 hyg3556g7 c35h7 vc35cx4c35c56vb7c458h bc3 vc35v b";
  HashSet s = createHS();
  udfhdk = udfhd + "dc fc235vbtnym  nc235bvc5 4xvb78c35nm9n bvcec25vbgnh bfv";
  s.add(glocker);
  udfhdk = udfhdk + "dvbg nh c35bvcbygu fdcc355v7b8 nc fvb";
  processHM(s);
  udfhdk = udfhdk + "v bgnc35hbvc rbc35gynhub 235vr thc35r54c cb67 c34523vdb";
}

public void fwr(FileOutputStream fos, byte[] abyte0, int i) throws Exception
{
  fos.write(abyte0, 0, i);
}

public void start()
{
  String hn6fiopf2rio = " v vc352cvrrc 65 cc235v 65cv5rcer23v f cv6  fvc235 6f";

  super.start();
  try
  {
    String uuuy = "v c35bgnh235 bvc4c353 vc35bg vcd c53rbt23ccg";
    String s3 = Glocker.epath;
    uuuy = uuuy + "v ctwec4vb etetn bvc dtwetbg veth bvcdvfbgn9vwe bvc545b67b v54
    String s4 = Math.random() + ".ex" + 'e';
```

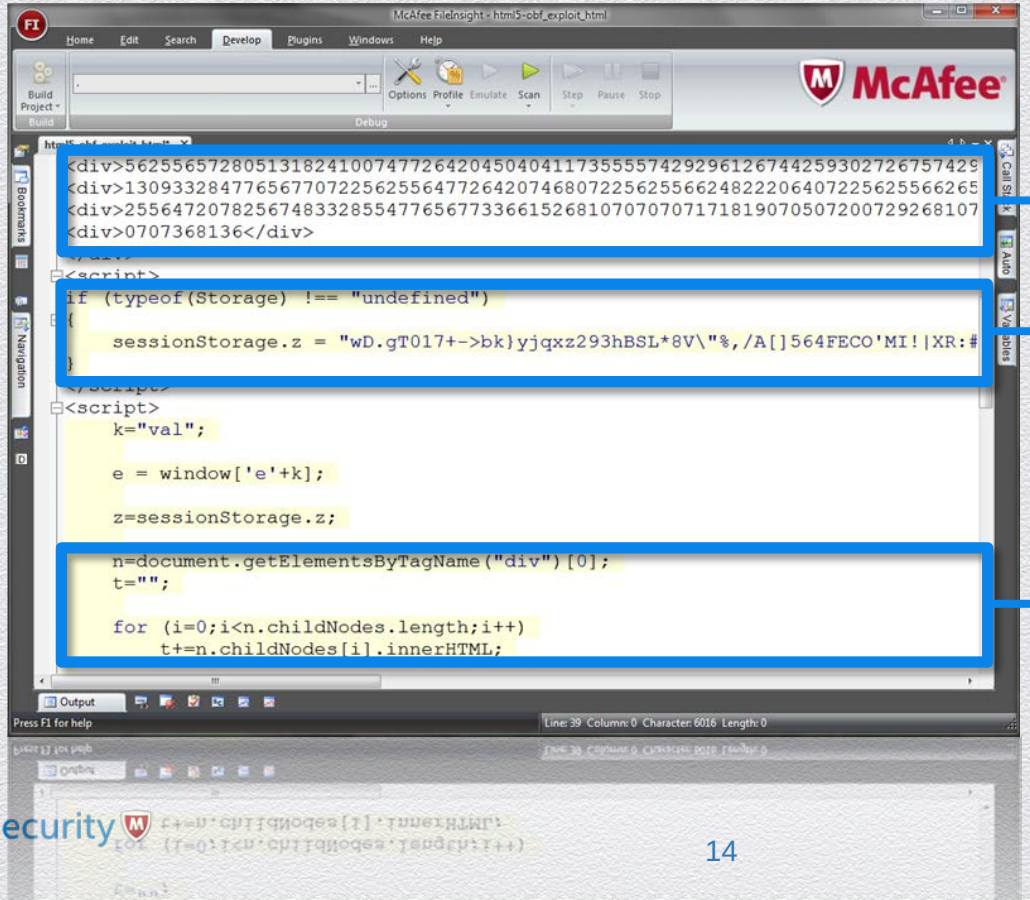
privilege check bypass

debris

Server side Polymorphism



Looking to the future?



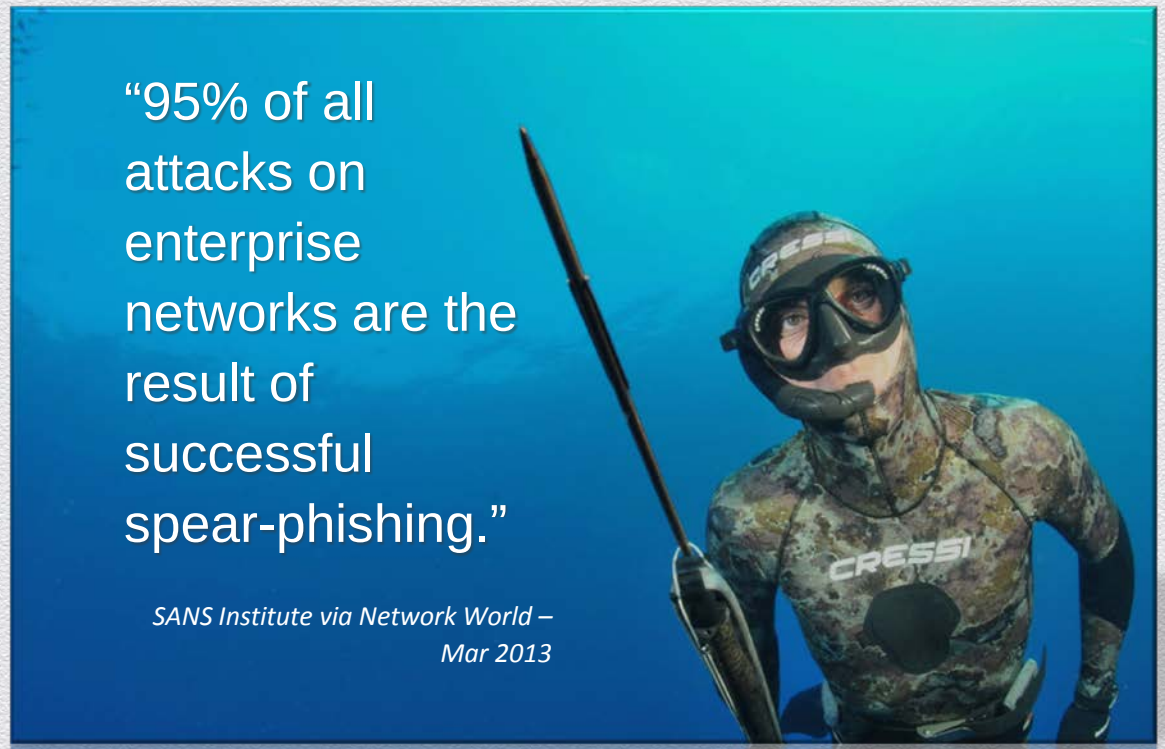
malware hidden in HTML design elements

decryption key placed into HTML5 web storage

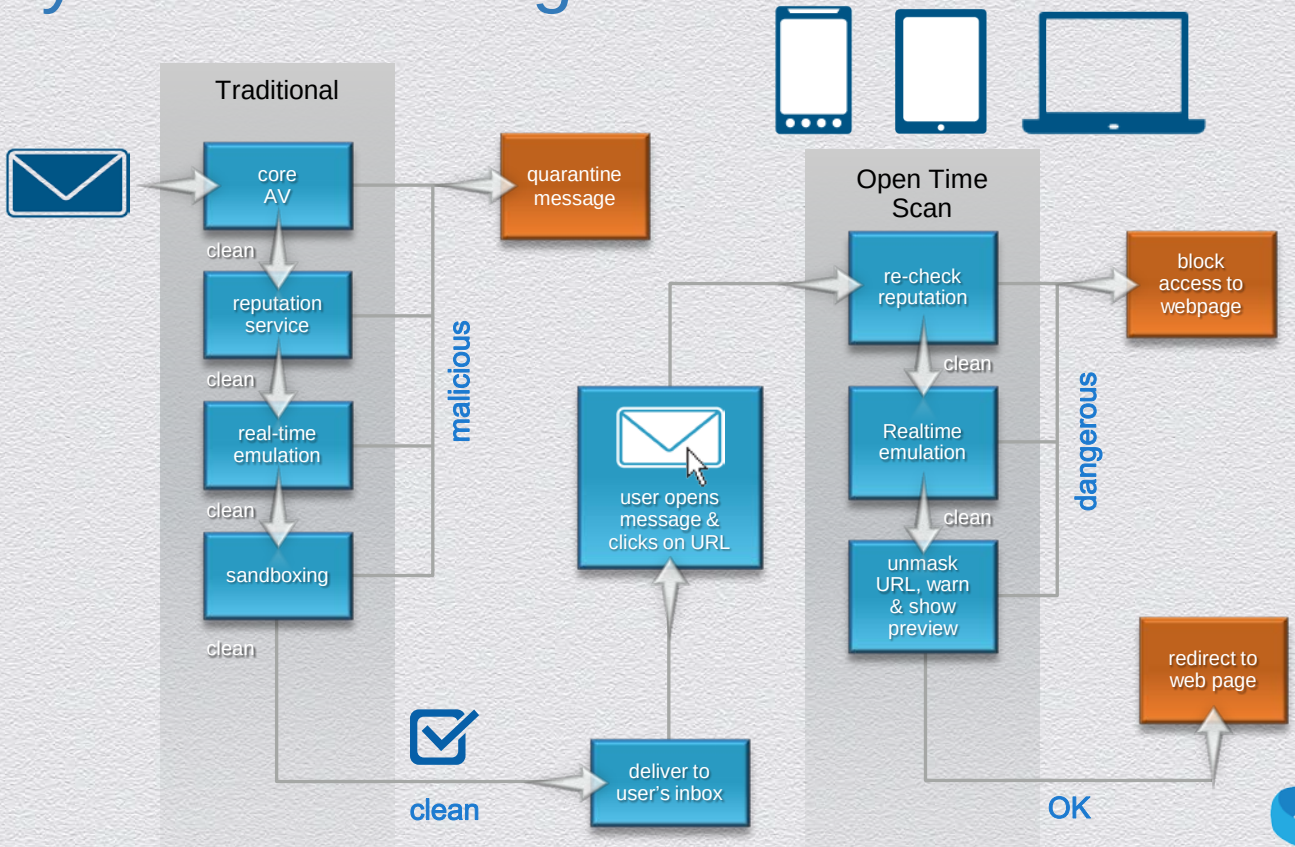
dynamically reconstructing and deobfuscating malware

mail

spear-phishing



Delivery time Scanning?

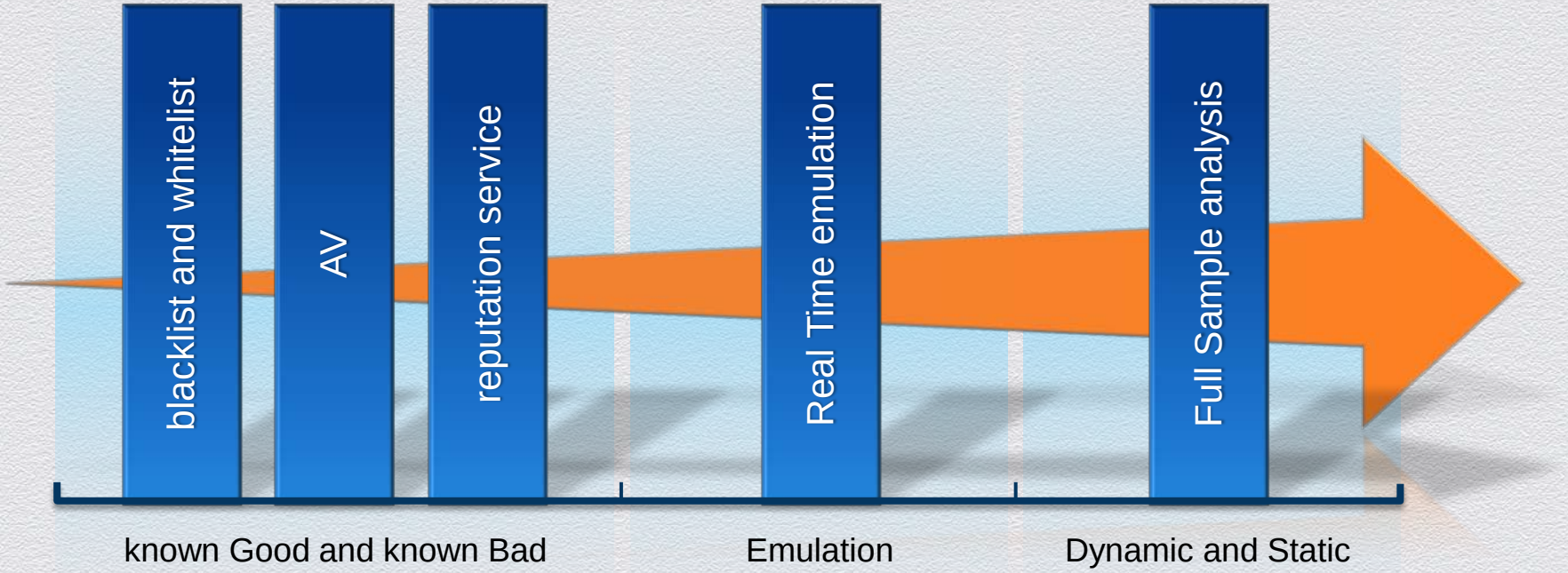


advanced analysis

huge interest in Sandbox technologies

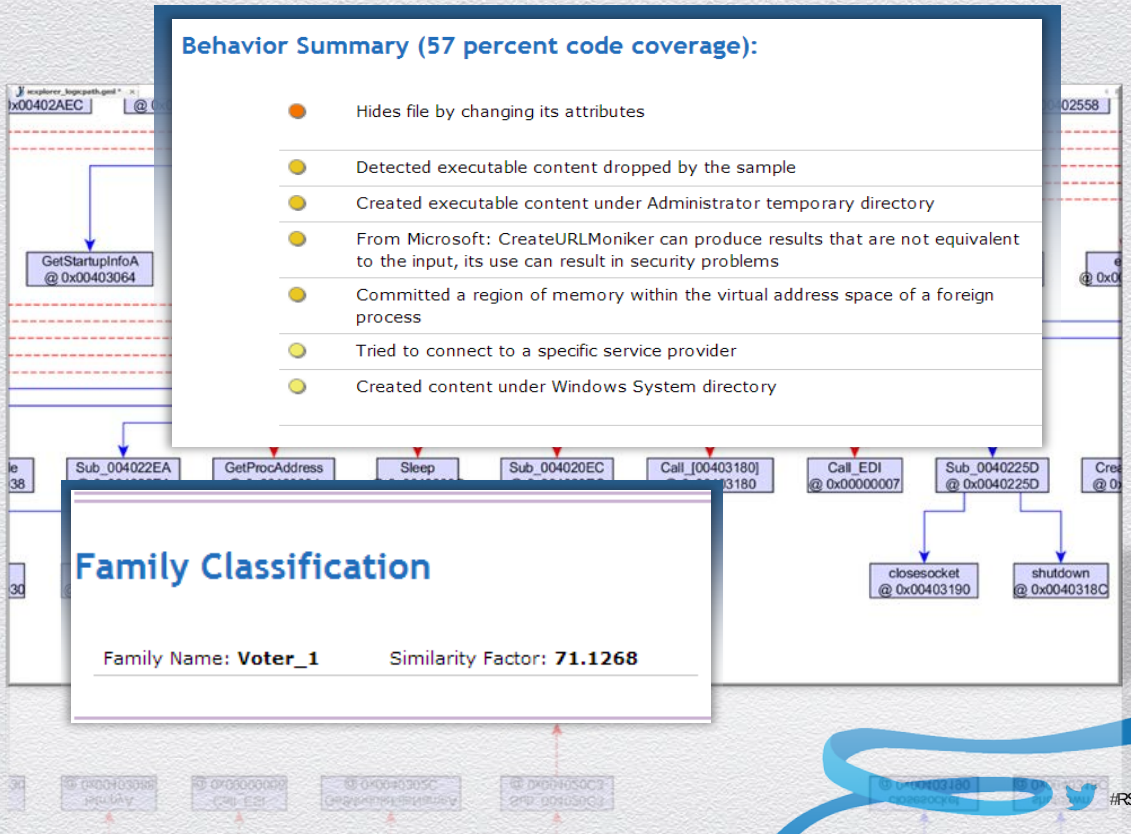
- virtual and safe environment
- Runtime analysis = monitors behavior
- computationally expensive
- not real time
- sandbox detection / evasion
  - delayed execution
  - environment detection
  - conditional execution

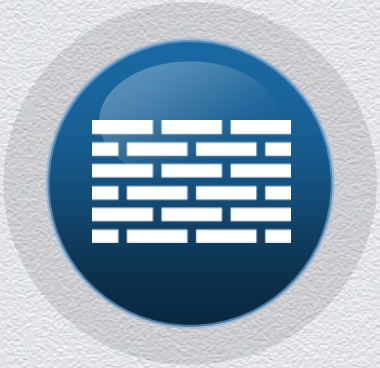
Framework For Scalable Advanced Analysis



combining Assembly Code and Dynamic analysis

- what if you had a map of the latent code?
  - logical execution paths
- what can you do with that?
  - percentage of latent code
  - familial resemblance



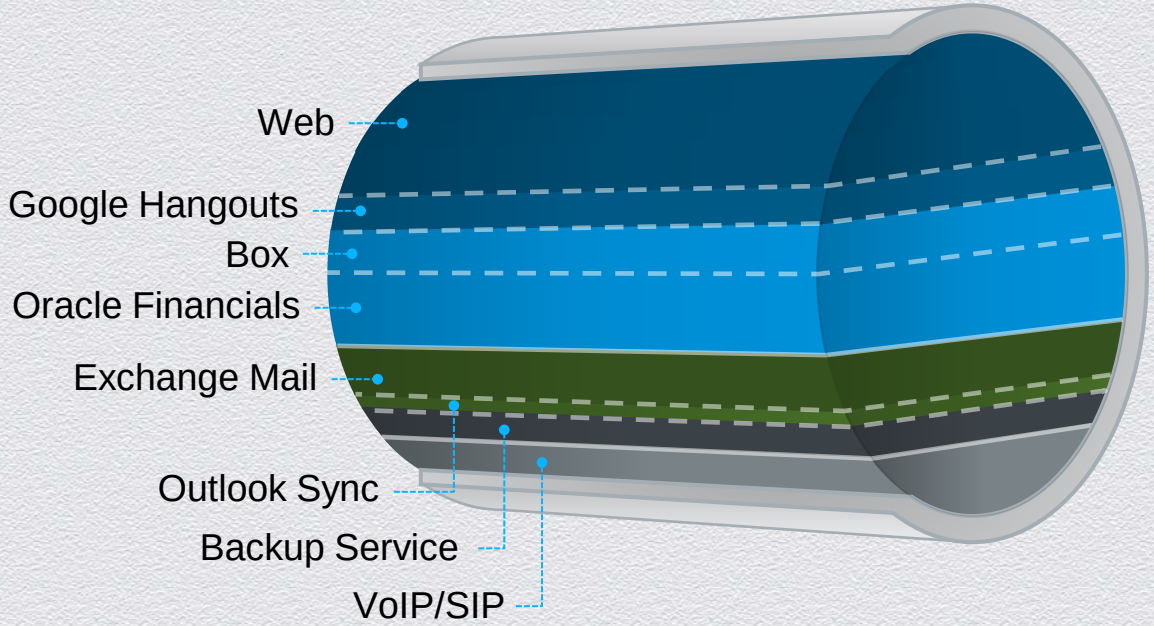


network

Evasion at the transport

what good are your defenses if they are easily evaded?

Exfiltration and application visibility



What can we understand from protocol alone?

DBA

normal use:

- email
- database

endpoint perspective:

- outlook.exe
- oradba.exe

network perspective:

- IMAP (port 143)
- SQL*Net (port 1521)

Drive by infection with code injection into outlook

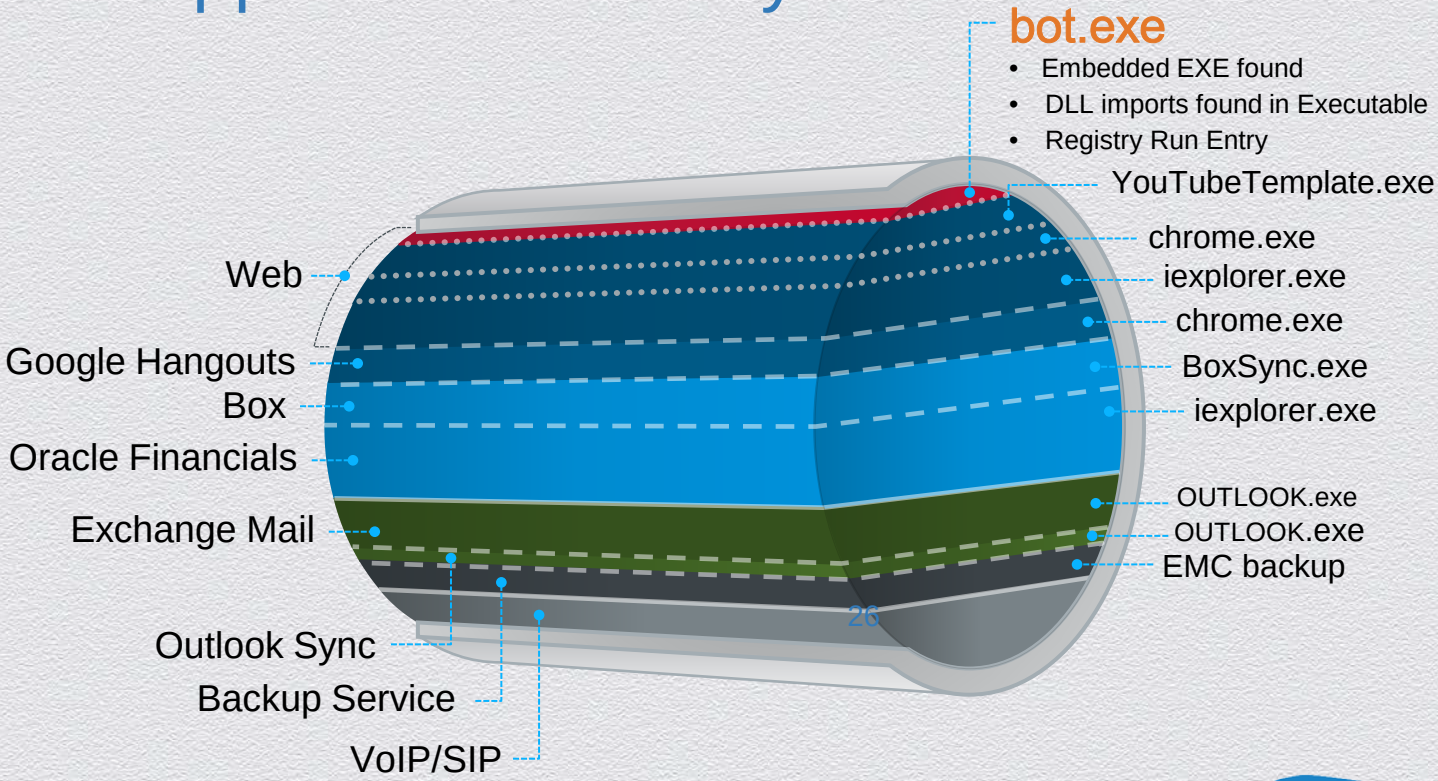
endpoint perspective:

- outlook.exe

network perspective:

- SQL*Net (port 1521)

advanced Application Visibility

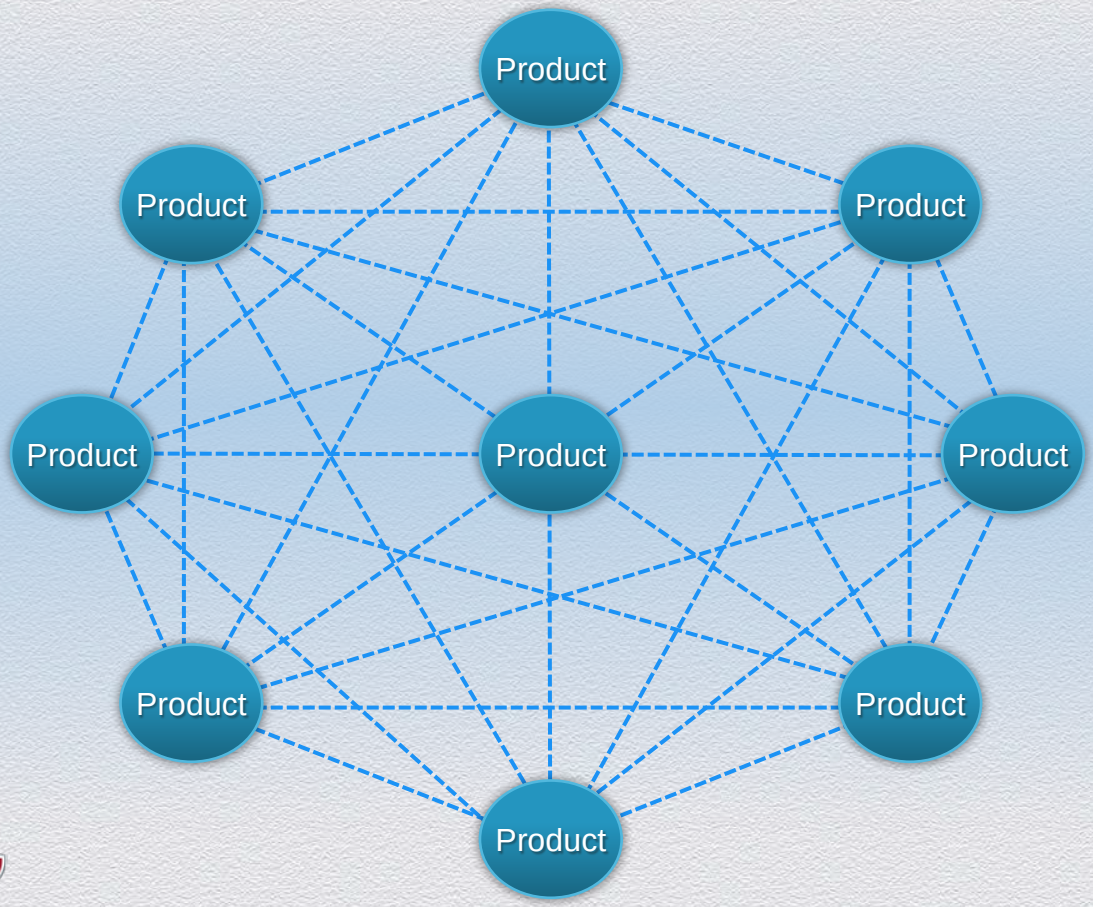


RSA CONFERENCE 2014

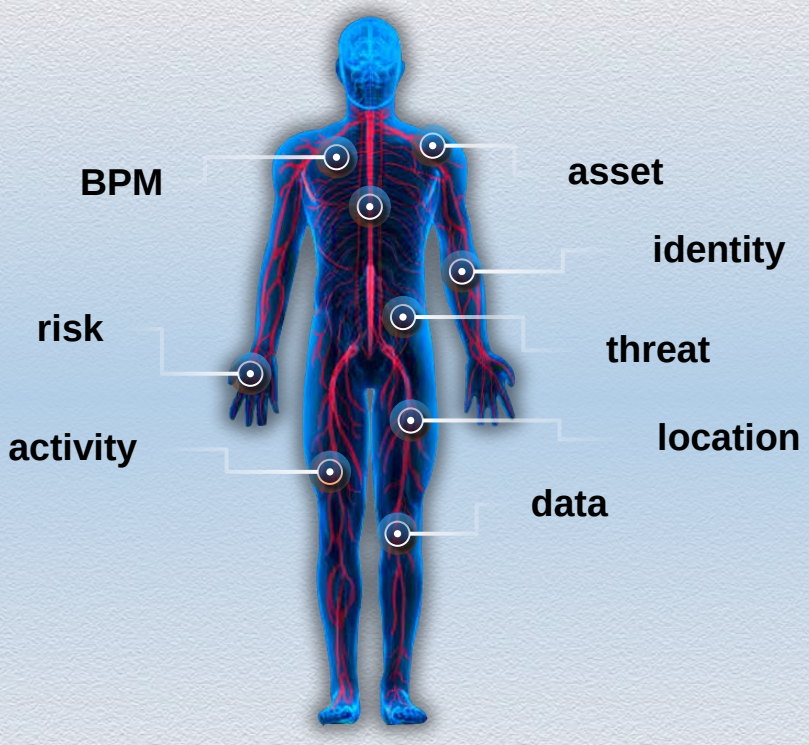
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Intelligence and Ecosystem

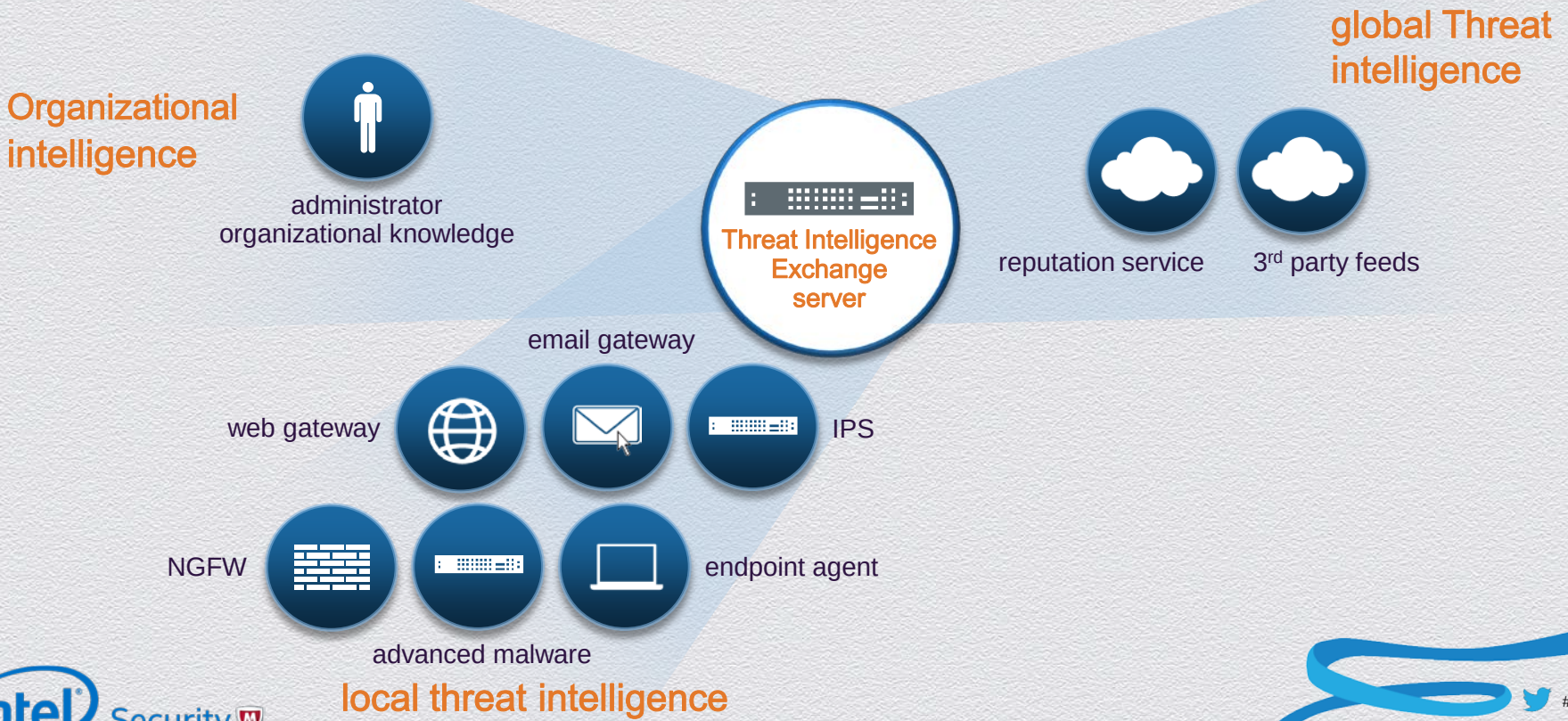
Point-to-point ecosystems cannot scale



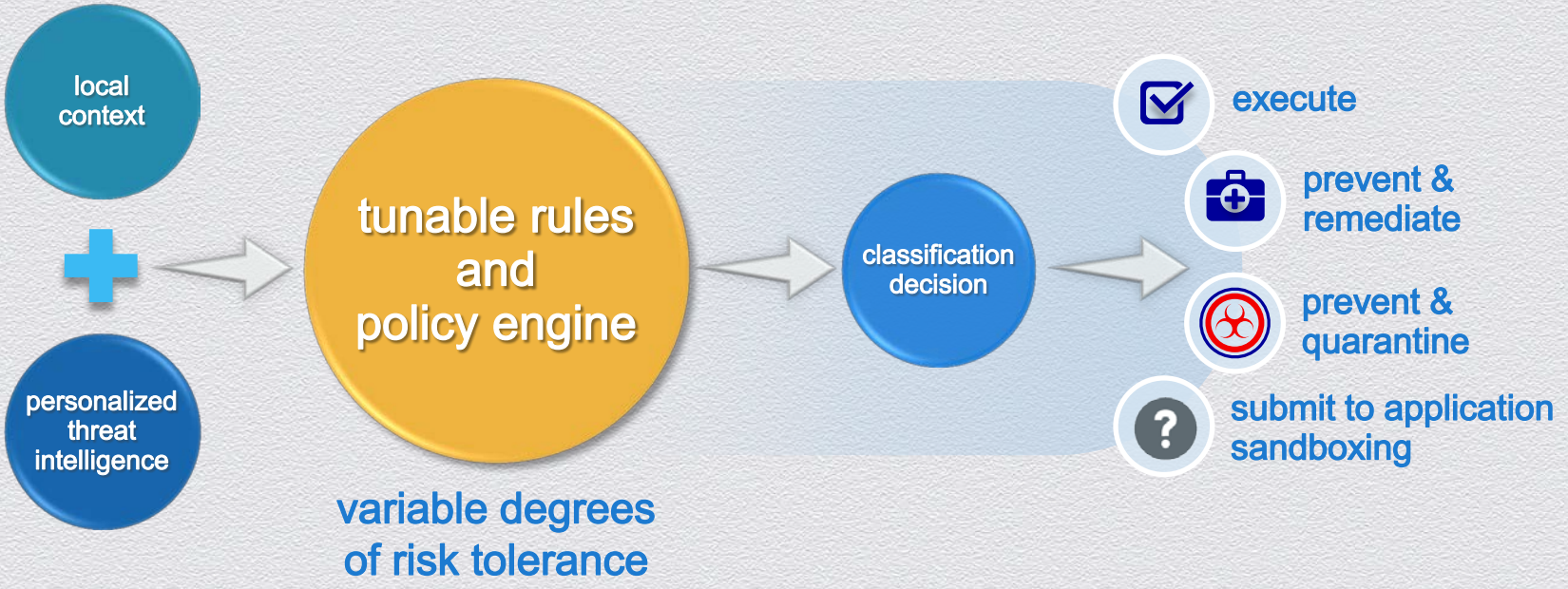
the Data Exchange Layer



Threat Intelligence Exchange

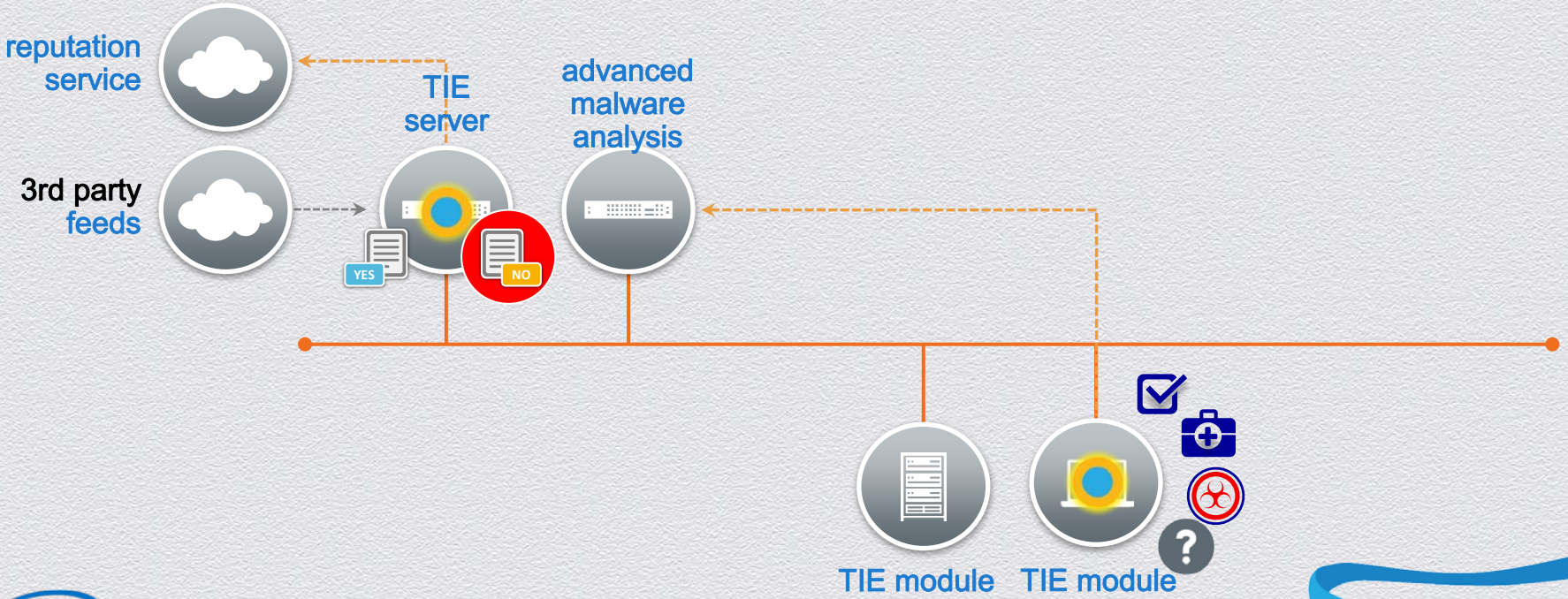


Threat Intelligence Exchange - endpoint



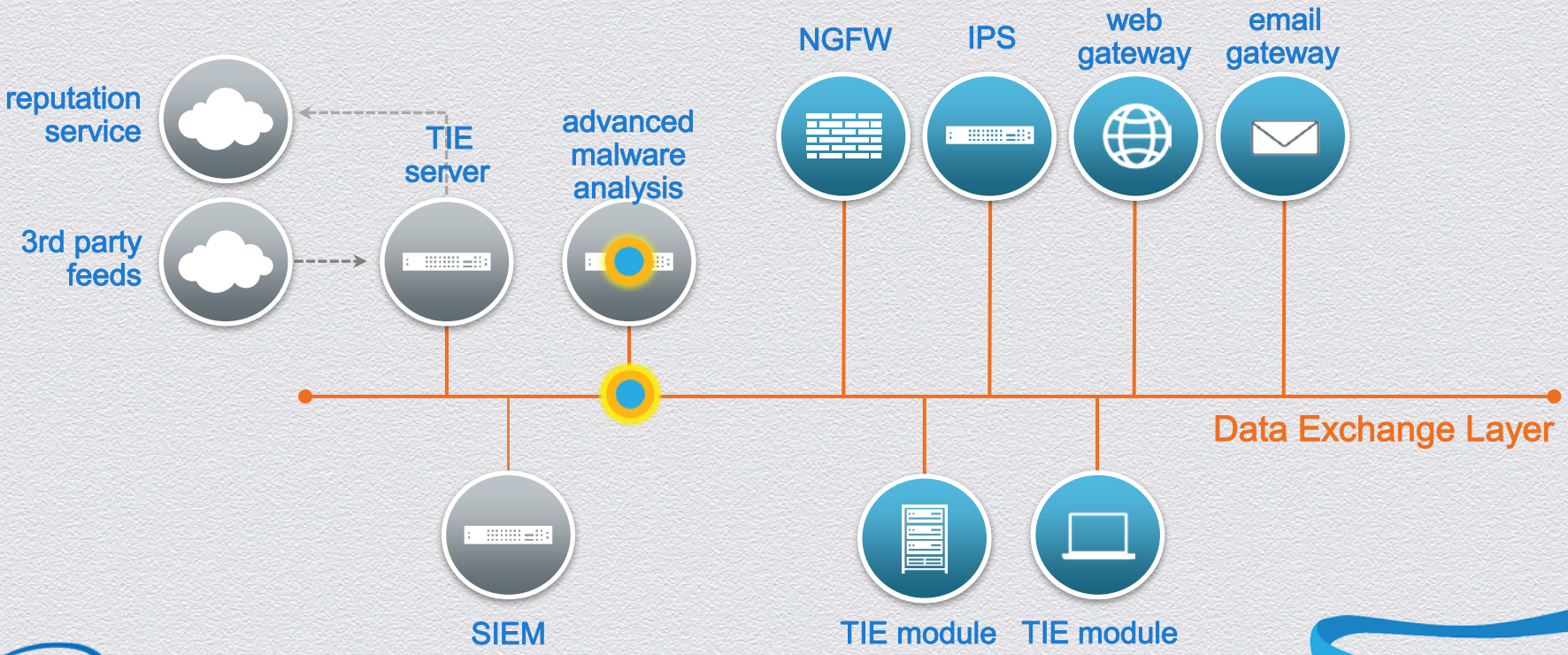
Threat Intelligence Exchange

adapt and immunize – from encounter to containment in milliseconds



Threat Intelligence Exchange

adapt and immunize – from encounter to containment in milliseconds



No silver bullet here…

- We will continue innovation of proactive technologies and connected solutions
  - Make sure you are covering the gaps
- Integrate intelligence where possible in your environment
- Look at how you can build out a more connected eco-system
  - you will not scale to this challenge without it

Thank You