



Mehmet Dağdevirentürk – Revolution at Endpoint Security

Endpoint Protection Problems



80%

Had network
attacks or exploits

KNOWN BAD

KNOWN GOOD

Years ago, the threat landscape was black and white

KNOWN BAD



Anti Malware



Blacklisting



Whitelisting



Application
Control

A number of classic threat defense techniques tackle these



Content
Filtering



Encryption

UNKNOWN



Zero-day attacks



Ransomware

Now, the “grey” is growing and is much harder to defend against



*Business Email
Compromise*



*Lateral
movement*



*Targeted
attacks*



Only 60% seconds

of malware only profits are
alive with ransomware hour

Machine Learning

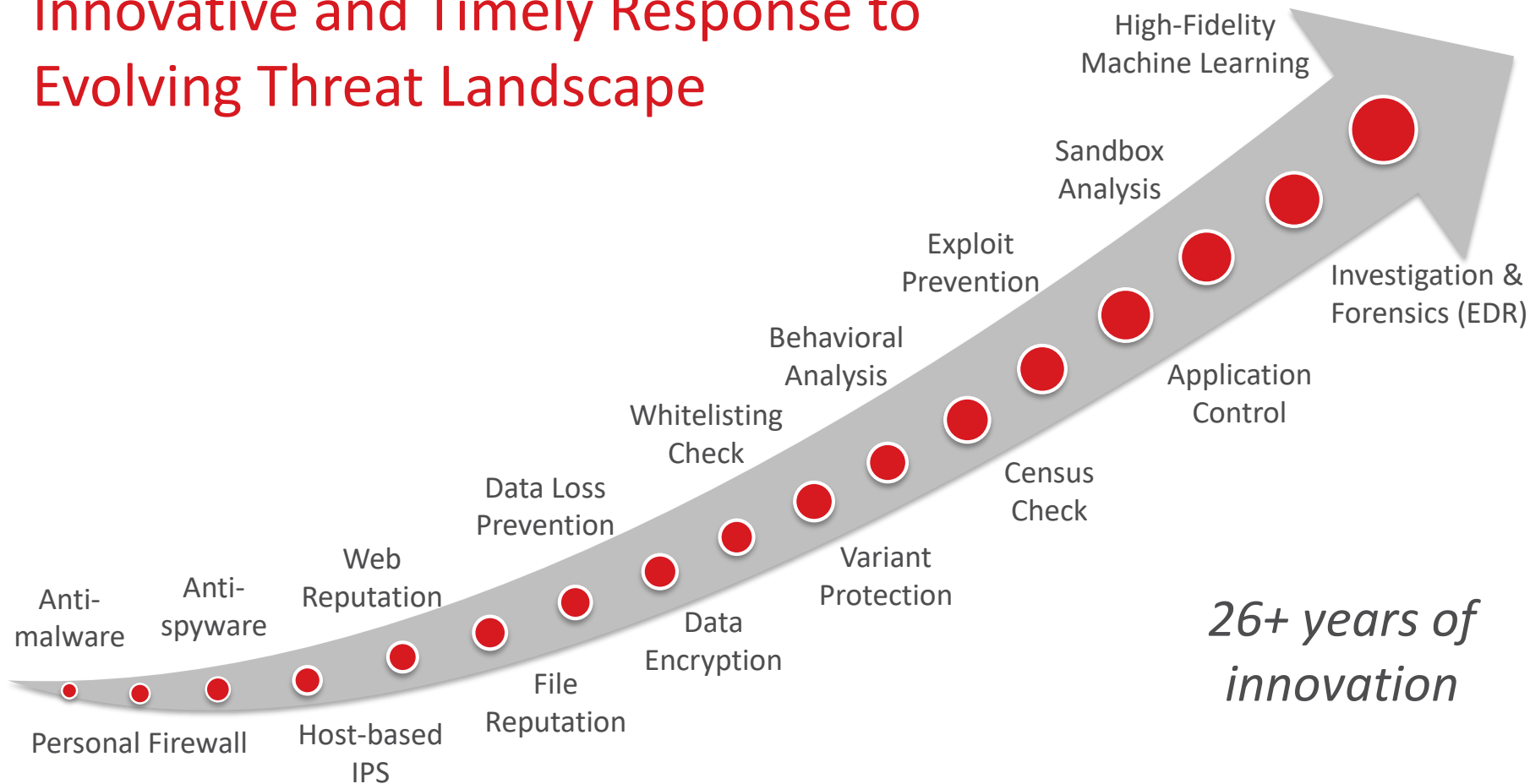
There is no silver bullet...



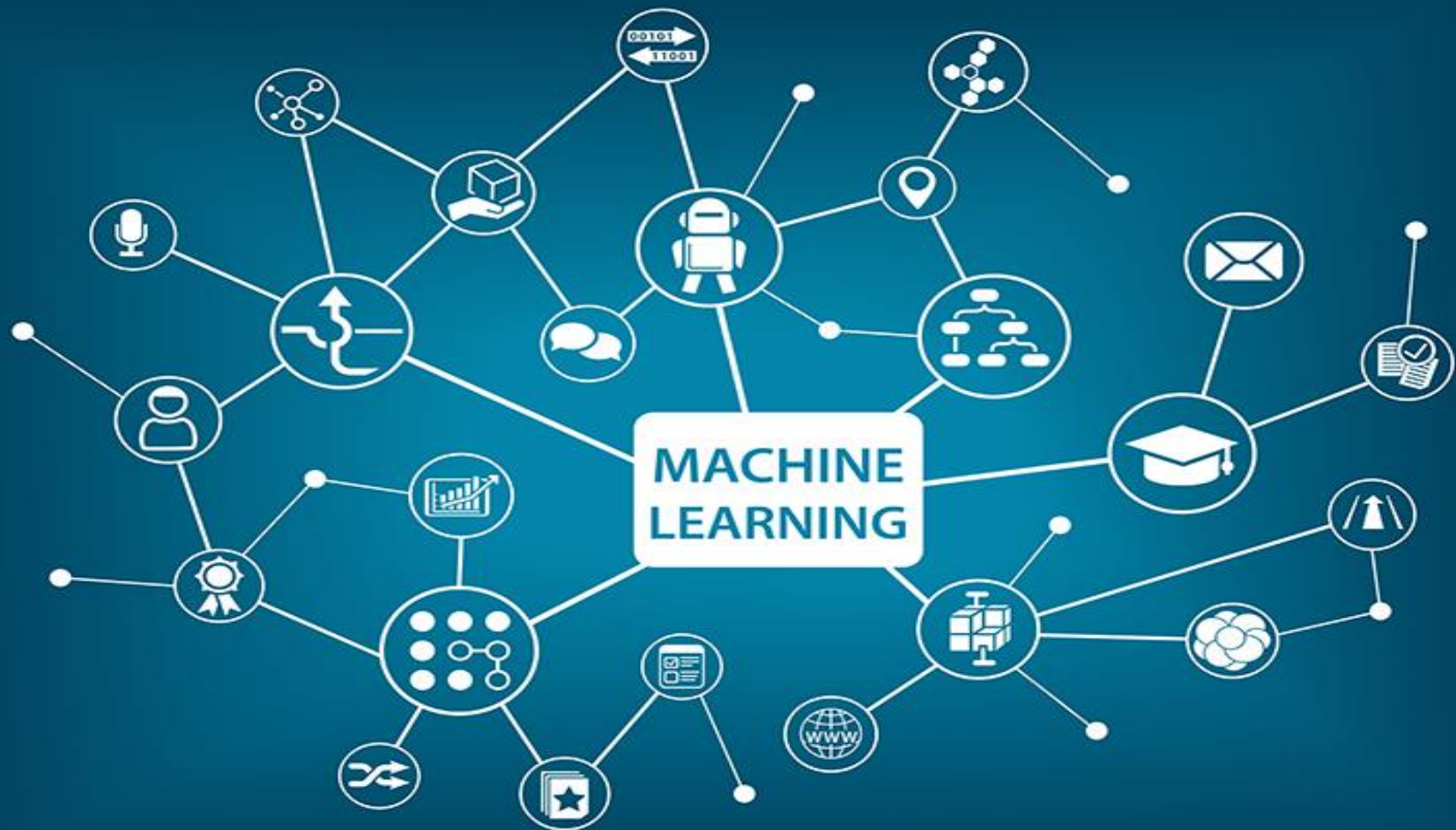
“History has clearly shown that no single approach will be successful for thwarting all types of malware attacks. Organizations and solution providers have to use an adaptive and strategic approach to malware protection.”

- Gartner EPP Magic Quadrant 2016

Innovative and Timely Response to Evolving Threat Landscape



*26+ years of
innovation*



Machine Learning Evolved



Spam Detection
2005



URL Reputation and
Categorization - 2010



File-based Threat
Detection

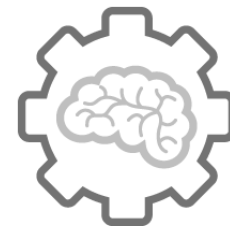


Endpoints
October 2016



Malicious Social Media
Accounts - 2015

High-fidelity Machine Learning



- Uses most accurate features to predict if a file is good or bad
- Unique dual approach for highest fidelity

Pre-execution Machine Learning

- Looks at static file features
- Reduces risk of damage
- Can miss features that only are seen during execution

Runtime Machine Learning

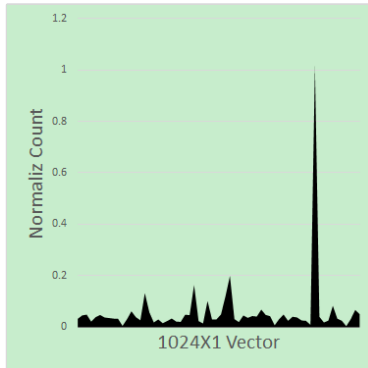
- Looks at behavior features during execution
- Kills offending processes during execution

Noise Cancellation Reduces False Positives:
Census and Whitelist Checking

Machine Learning Predicts Maliciousness

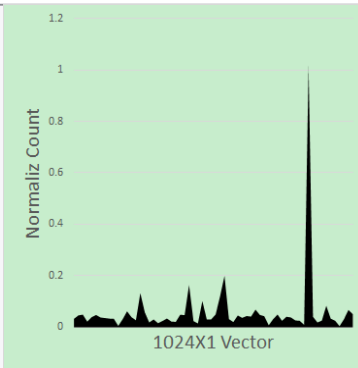
When features are looked at and compared

Ransom-Tescrypt3 (Known sample)

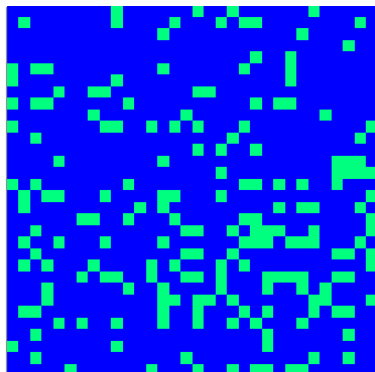


Opcode –
normalized
in graph

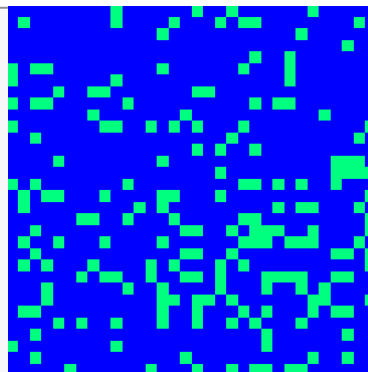
Ransom-Tescrypt4 (Unknown)



Example of 2 code
elements machine
learning found to
have similar
characteristics



API calls –
displayed in
import table



Why Machine Learning

Samples Look Different on the Surface

Ransom-Tescrypt1 (Known sample)

```
mov     ecx, [ebp-38h]
add     ecx, 1E6h
mov     edx, [ebp-2Ch]
sub     edx, ecx
mov     [ebp-2Ch], edx
mov     eax, [ebp-18h]
sub     eax, 2CEh
test    eax, eax
jz      short loc_41DFAB
```

```
mov     ecx, [ebp-38h]
add     ecx, [ebp-38h]
mov     edx, [ebp-18h]
sub     edx, ecx
mov     [ebp-18h], edx
mov     eax, [ebp-18h]
add     eax, 16Ah
[ 3 instructions deleted ]
mov     edx, [ebp-38h]
mov     eax, [ebp-18h]
lea     ecx, [eax+edx+288h]
```

Ransom-Tescrypt2 (Unknown)

```
mov     eax, [ebp-0Ch]
add     eax, [ebp-0Ch]
```

```
|
test    eax, eax
jz      short loc_41E598
mov     ecx, [ebp-0Ch]
mov     edx, [ebp-0Ch]
lea     eax, [edx+ecx-3Fh]
[ 11 instructions deleted ]
mov     ecx, [ebp-38h]
add     ecx, [ebp-0Ch]
test    ecx, ecx
jz      short loc_41E5D1
```

```
mov     edx, [ebp-38h]
add     edx, 5Bh
mov     eax, [ebp-0Ch]
```


Unknown threat found by machine learning


Log Details

Ransom.Win32.TRX.XXPE1

 29/09/2016 22:11:24
Terminate

 Sample002.exe

 nwadmin
V06WKS001
192.168.100.151

 Local or network drive
C:\Falcon\

Threat Indicators

File Details

Threat Probability

95%

Probable Threat Type

Ransomware

Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features.

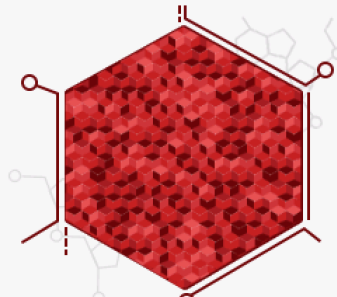
Threat Identifiers

The file uses the following API function calls, which indicate one reason that this file may contain an unknown threat.

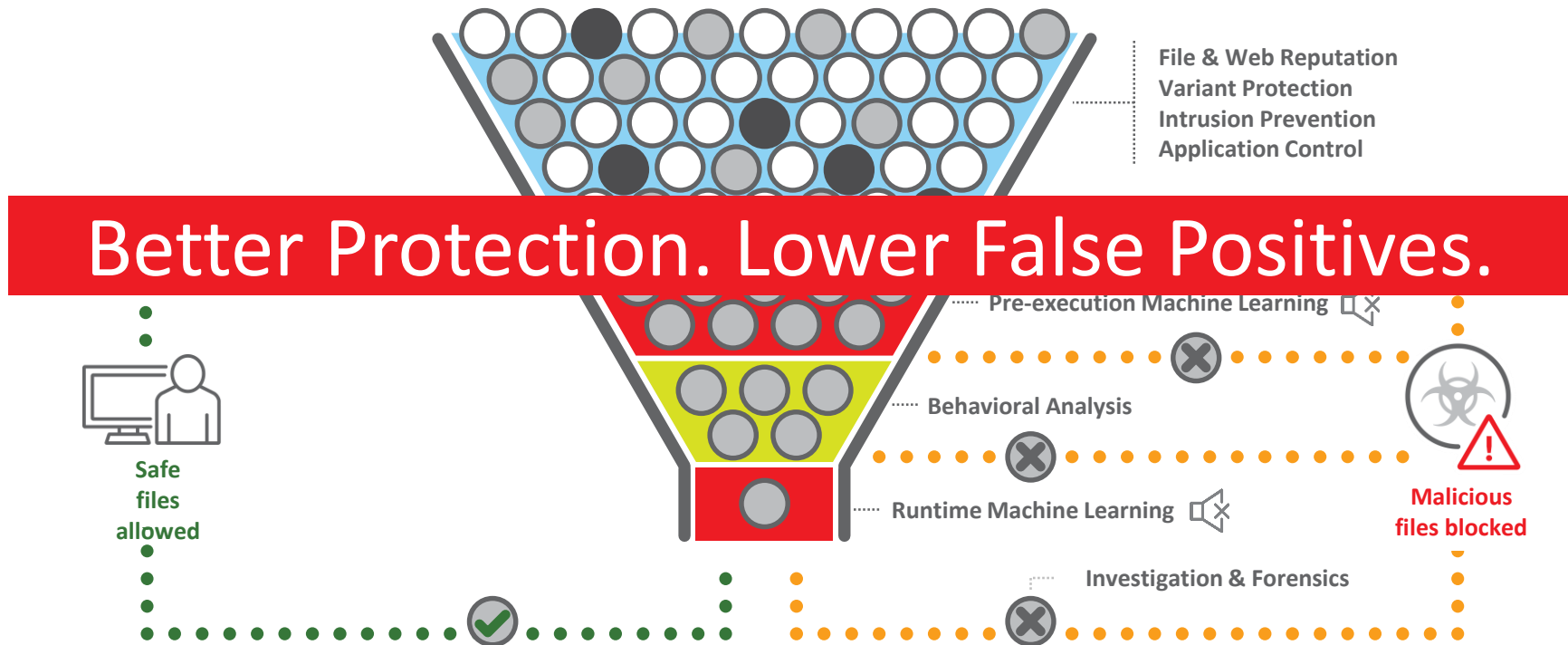
- CopyFileW
- CreateFileA
- CreateFileMappingW
- CreateFileW
- CreateMutexW

Similar Known Threats

[Ransom_CERBER.BZC](#)
[Ransom_CERBER.C](#)
[Ransom_CRYPNISCA.SM](#)

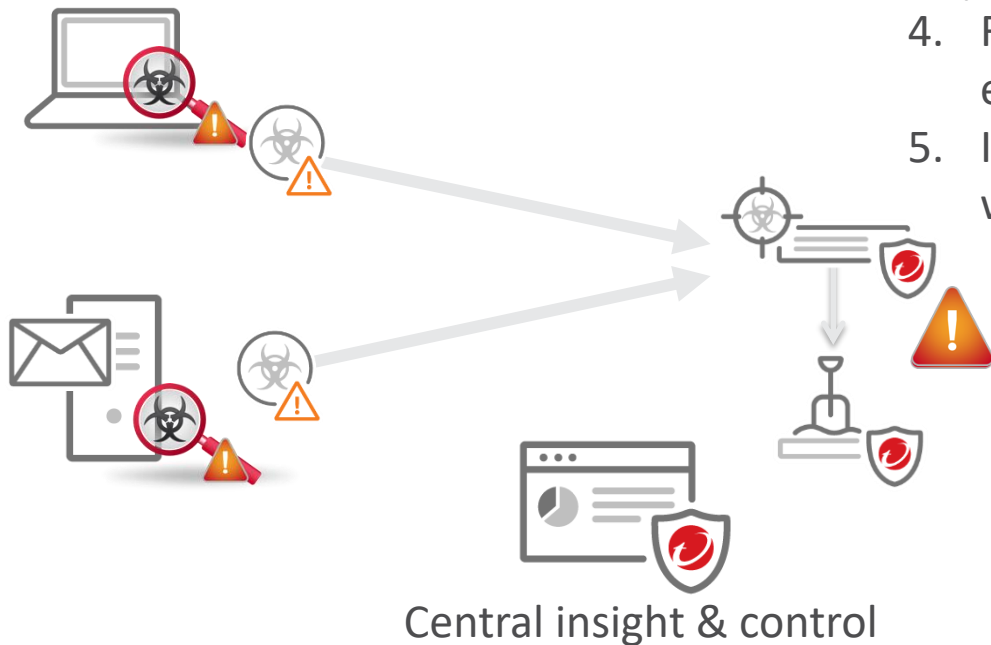


Trend Micro – Max Protection with The Right Technique At The Right Time



Security That Automatically Adapts

1. Advanced malware attempts to infect an endpoint
2. Sent to network sandbox for assessment
3. Sandbox sends alert back to endpoint (for blocking)
4. Real-time signature pushed to all endpoints and gateways
5. Investigation determines if and where the threat has spread



Central Visibility

[Back](#)

User - GREENTHIS\Administrator

[Help](#)

[Security Threats](#) [Policy Status](#) [Contact Information](#)

Security Threats Over Time



Zoom [1d](#) [1w](#) [2w](#) [1m](#)

09-04-2016 ~ 10-04-2016

V04SVR001

V06WKS001

V06WKS007

GREENTHIS\Administrator

OSCE12-BETA

Date: 09-15-2016

Suspicious File:

31EB992A491AF1400E43C832A96AE50A33D7D7C1(1)
43633571279F7825A35973D7BB522A49F546AF94(1)
1F086CBE6DC1353A0A1C6D5C5836ACCD19FD4B0D(1)
and 3 more unique violation(s)

Predictive Machine Learning Detection:
Ransom.Win32.TRX.XXPE1(2)



Security Threat Details

Security Threat	Category	File Path / Email Subject / Rule Name	Action	Endpoint	Logged by	Time	Details
Troj.Win32.TRX.XXPE0005	Predictive Machine Learn...	c:\users\inwadmin\downloads\malwaresampl...	Quarantine succe...	V06WKS001	OfficeScan	10/03/2016 07:23:34 PM	View
Troj.Win32.TRX.XXPE0005	Predictive Machine Learn...	c:\users\inwadmin\appdata\local\microsoft\wi...	Quarantine succe...	V06WKS001	OfficeScan	10/03/2016 07:23:32 PM	View
Ransom.Win32.TRX.XXPE1	Predictive Machine Learn...	c:\users\inwadmin\downloads\trendx_detect...	Quarantine succe...	V06WKS001	OfficeScan	10/03/2016 05:06:00 PM	View
Ransom.Win32.TRX.XXPE1	Predictive Machine Learn...	c:\users\inwadmin\appdata\local\microsoft\wi...	Quarantine succe...	V06WKS001	OfficeScan	10/03/2016 05:05:57 PM	View
Ransom.Win32.TRX.XXPE1	Predictive Machine Learn...	C:\Falcon\Sample002.exe	File passed	V06WKS001	OfficeScan	09/29/2016 10:57:52 PM	View

2017 Magic Quadrant

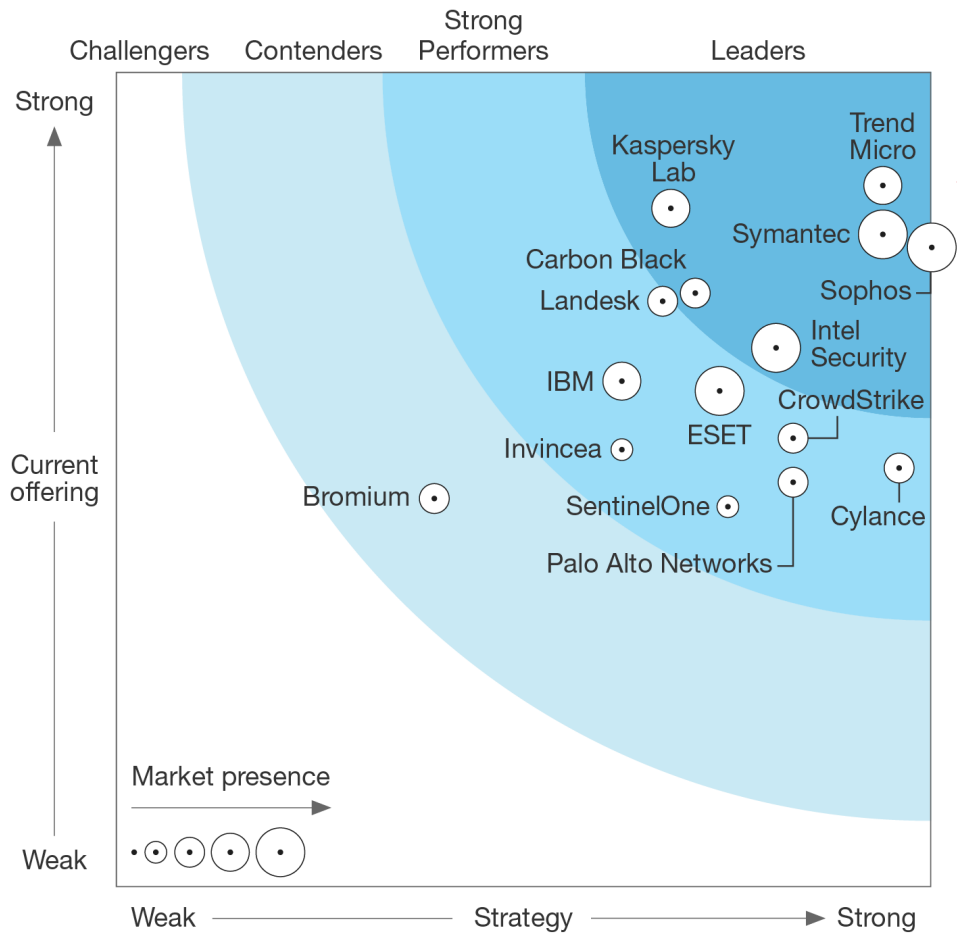
Gartner Magic Quadrant for Endpoint Protection Platforms

Jan. 30, 2017

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from <https://resources.trendmicro.com/Gartner-Magic-Quadrant-Endpoints.html>

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.





FORRESTER®

Forrester Wave: Endpoint Security Suites, Q4 '16

THANK YOU

