



**Check Point**  
SOFTWARE TECHNOLOGIES LTD

**CPX  
360**

# SANDBLAST 2020

A quantum leap in threat prevention

Eytan Segal, Head of Product Management

WELCOME TO THE FUTURE OF CYBER SECURITY



Can you detect if your food is **poisoned**?





Can you detect if  
your **food** is poisoned?

### ZERO DAY POISON

locane Powder

- Odorless
- Tasteless
- Dissolves instantly
- **Deadly**

Can you detect if  
your **email** is poisoned?


### ZERO DAY MALWARE

- Signature-less
- Fileless
- Acts instantly
- **Devastating**





# What was 2019 like?



**42%** of malware is unknown

**33%** increase in mutations

**AVERAGE ORGANIZATION, EVERY DAY**

**42 malwares** are downloaded

**720 malicious websites** are accessed

**7,200 vulnerability exploits** are attempted

**2019**

Data from Check Point ThreatCloud

# Over 70 US local governments hit by **ransomware** in 2019



**Baltimore government held hostage by hackers' ransomware**

May 2019

*The New York Times*

**Ransomware Attack Hits 22 Texas Towns, Authorities Say**

Aug 2019

**WIRED**

**Ransomware Hits Georgia Courts as Municipal Attacks Spread**

July 2019

*The New York Times*

**Hit by Ransomware Attack, Florida City Agrees to Pay Hackers \$600,000**

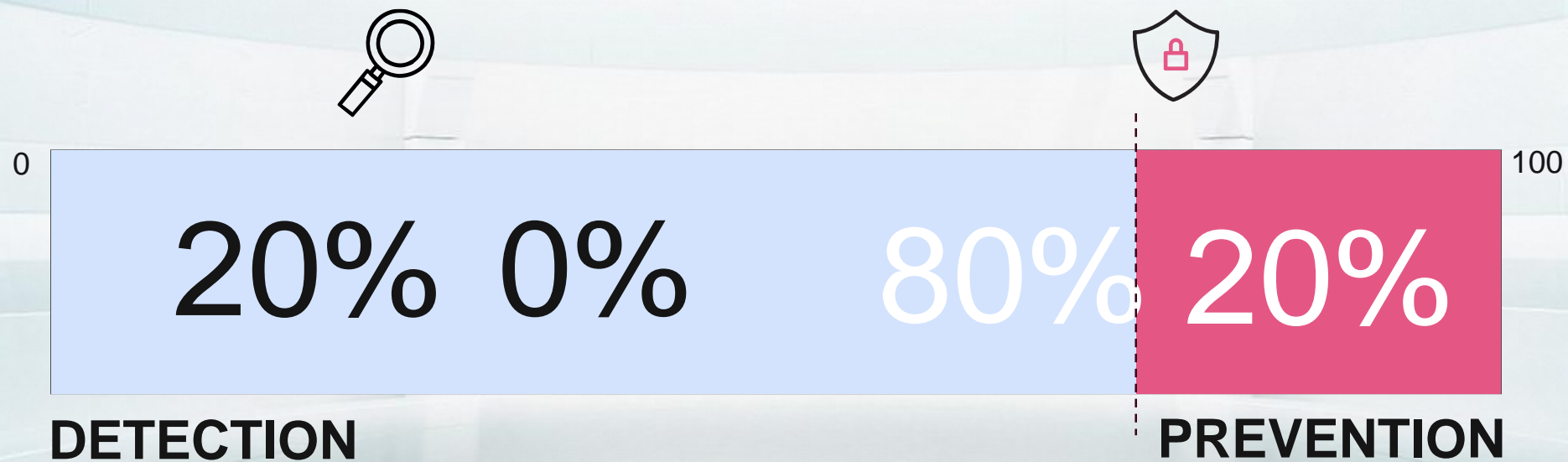
June 2019





**CAN WE MAKE 2020 BETTER?**





# PREVENTION FIRST

# HARNESS THE POWER OF TECHNOLOGY

ADVANCED TECHNOLOGY



BLOCK ZERO-DAY THREATS

AI

Behavioral  
Analysis

Threat  
Intelligence

CPU-level  
Sandbox



Phishing

Malware

Exploits

Ransomware





# PRODUCT FAMILY

The only solution to  
**prevent zero-days** in real time

NETWORK



Web, Mail &  
Data Center

AGENT



Endpoint &  
Browsers

MOBILE



iOS &  
Android

CLOUD



SaaS &  
IaaS

<API>

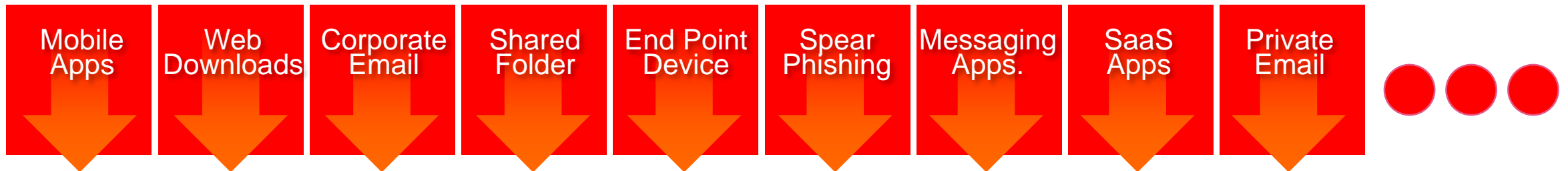


Integrate with  
any application





# PREVENT ALL ATTACK VECTORS



# 2019 NSS Labs BPS Test



Check Point  
SOFTWARE TECHNOLOGIES LTD

Breach Prevention Systems 2.0

**HIGHEST  
SECURITY EFFECTIVENESS**



- 100% Block Rate
- 100% Protection against HTTP Malware
- 100% Protection against Email Malware
- 100% Exploit Resistant
- 100% catch-rate in post infection
- **98.4% Overall Security Effectiveness**
- 0.0% False Positives
- A Leading TCO: \$19 Price/protected Mbps

# SandBlast 2020

What's new?



# SandBlast 2020 – what's new?



**Fast  
Inline Prevention**



**Advanced  
Email Protection**



**Artificial  
Intelligence**

**The world's best zero-day prevention. Period.**



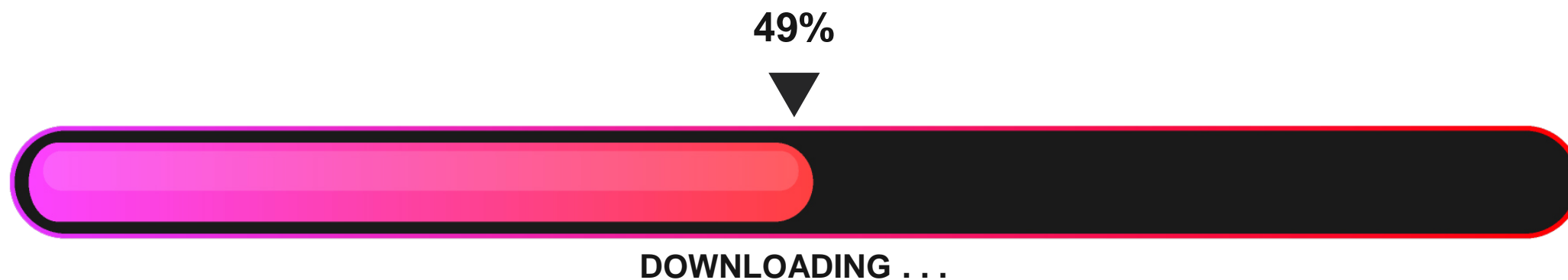
# FASTER THAN EVER!

Fast & accurate  
verdicts

=

Practical  
inline prevention

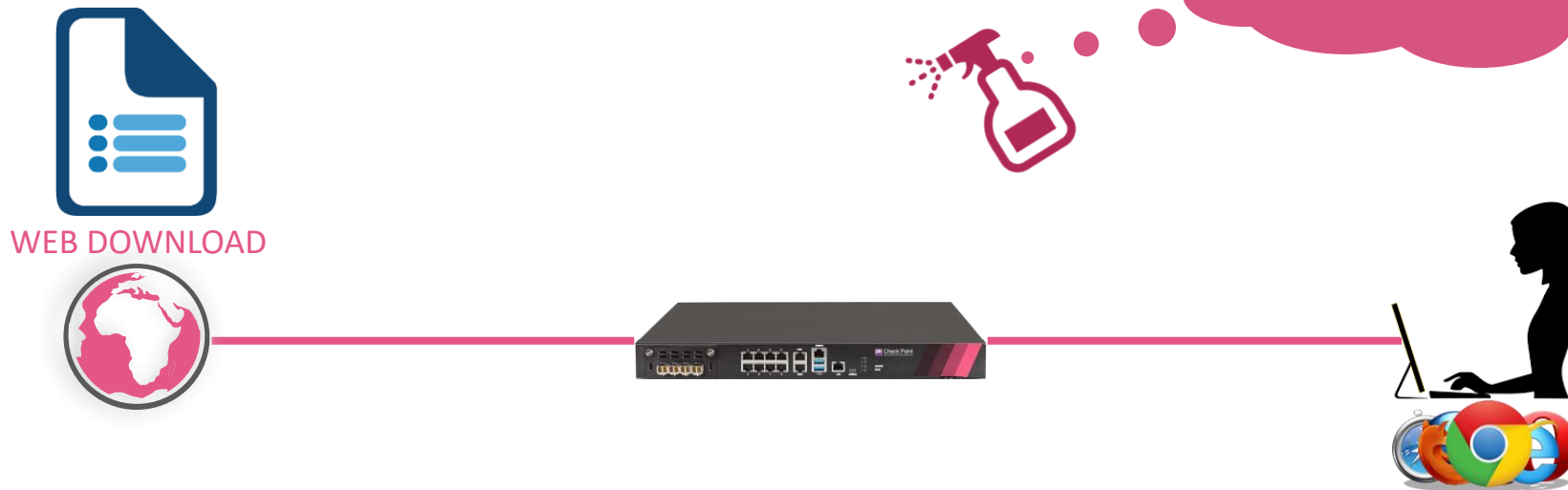
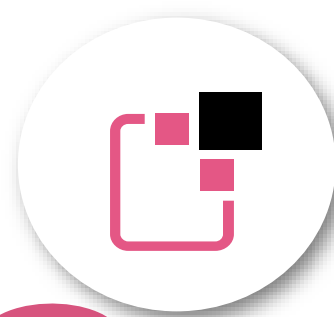
*We all hate waiting...*



it doesn't mean we should  
**compromise on security!**



# Rapid delivery of web downloads while PREVENTING ZERO-DAY MALWARE



➤ Clean files delivered in less than 3 seconds

**Unique** to Check Point!



# SandBlast 2020 – what's new?



**Fast  
Inline Prevention**



**Advanced  
Email Protection**



**Artificial  
Intelligence**

**The world's best zero-day prevention. Period.**



# Protecting your email with Check Point

Protect with  
**CloudGuard SaaS**

 Office 365

 Suite

Protect with  
**SandBlast Network**

  
Exchange

The background features a dark green color with vertical columns of glowing green text, resembling computer code or data. Two black silhouettes of hands are positioned on the left and right sides, appearing to reach towards the center. A semi-transparent dark green horizontal band is overlaid across the middle of the image, containing the main text.

Most **successful** attacks  
start with an **email**

**WHY?**

# WHY IS EMAIL SO DANGEROUS?

1

Threat actors can  
**approach anyone**

*Anyone can send you an  
email*

2

Extremely hard to  
**detect accurately**

Malicious Attachments

Malicious Links

Phishing

3

The  
**human element**

*Social engineering works...*



# Prevent **zero-day** email attacks with **SandBlast**

2

Extremely hard to  
**detect accurately**

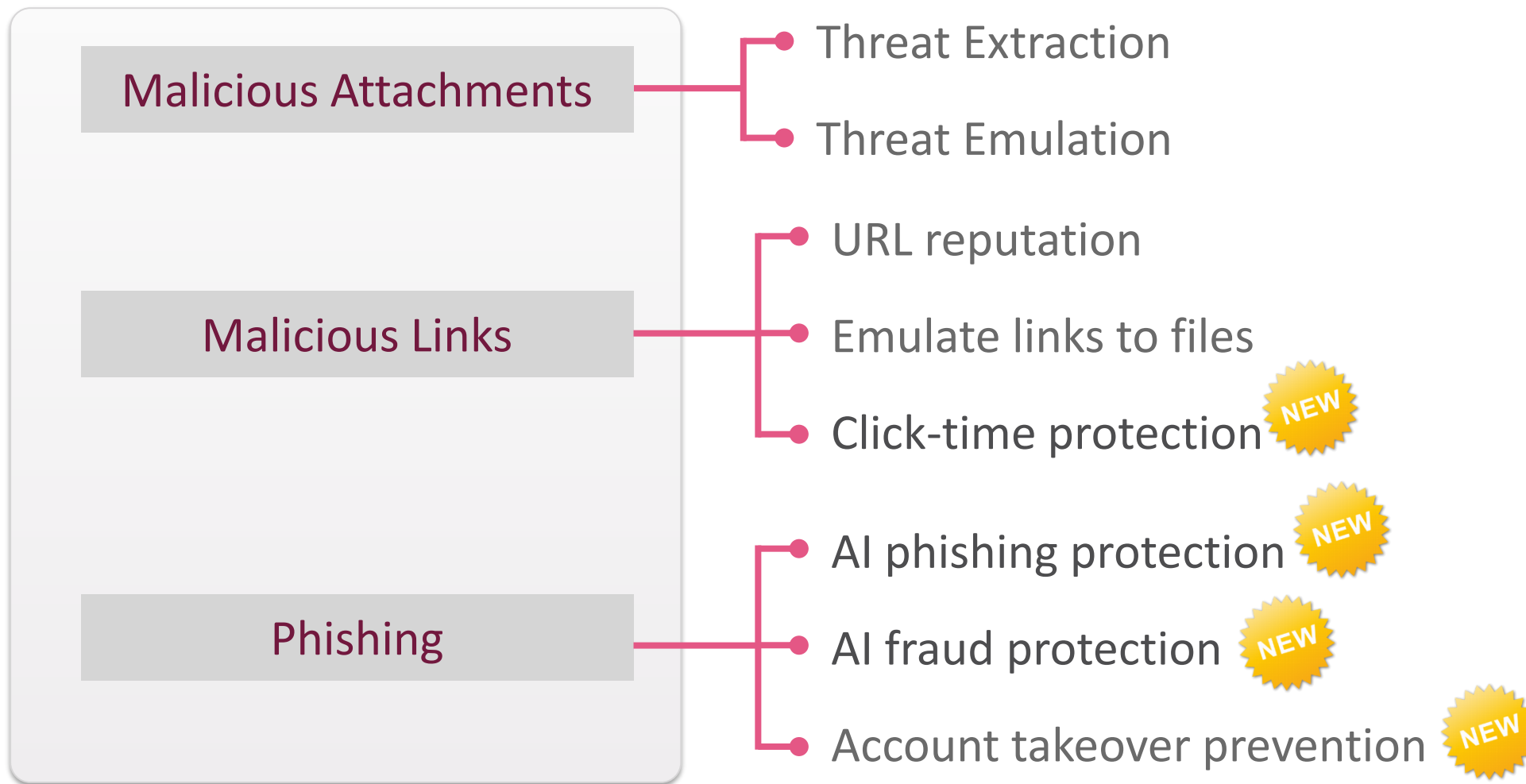


Malicious Attachments

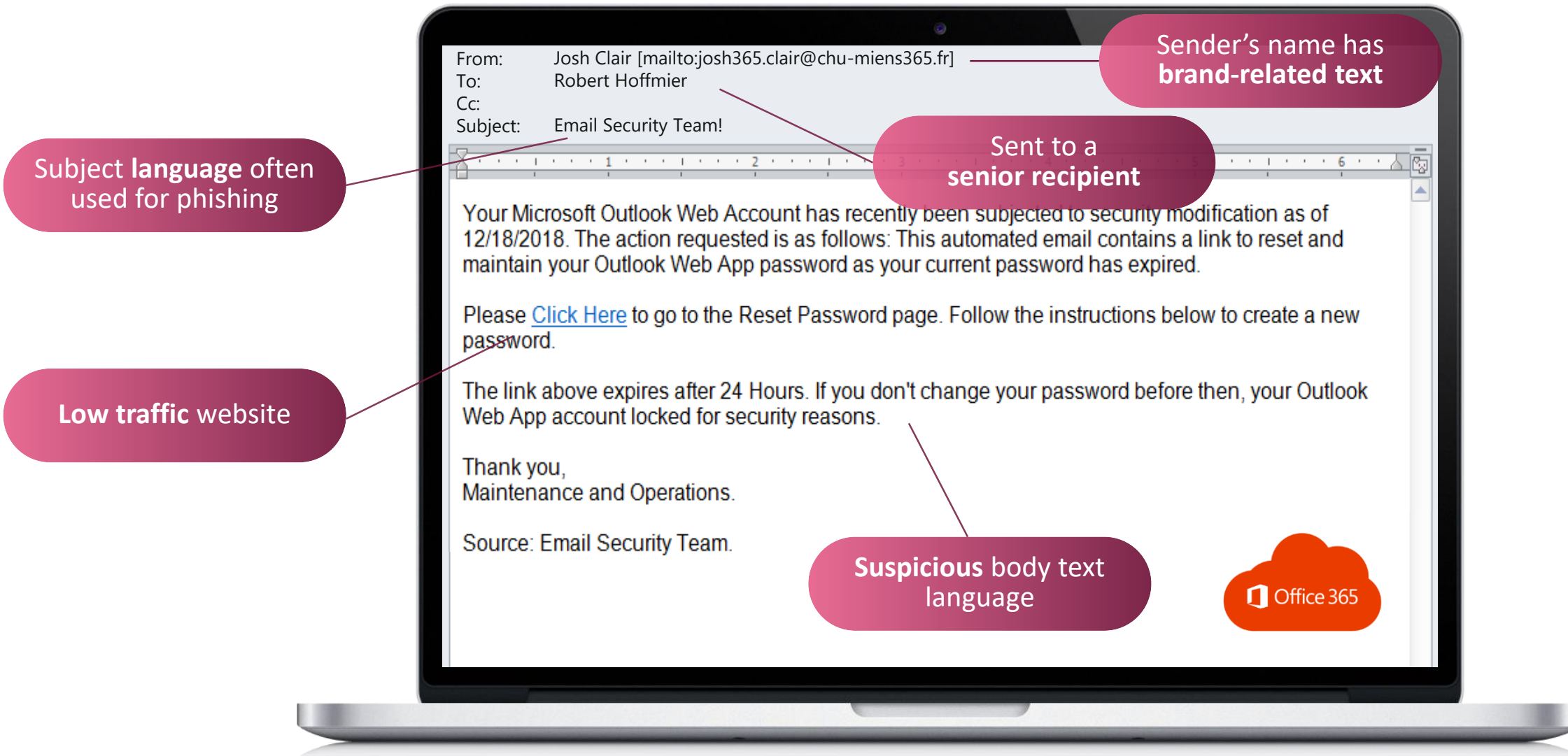
Malicious Links

Phishing

# Prevent **zero-day** email attacks with **SandBlast**



# WHAT'S WRONG WITH THIS MAIL?



From: Josh Clair [mailto:josh365.clair@chu-miens365.fr]

To: Robert Hoffmier

Cc:

Subject: Email Security Team!

Your Microsoft Outlook Web Account has recently been subjected to security modification as of 12/18/2018. The action requested is as follows: This automated email contains a link to reset and maintain your Outlook Web App password as your current password has expired.

Please [Click Here](#) to go to the Reset Password page. Follow the instructions below to create a new password.

The link above expires after 24 Hours. If you don't change your password before then, your Outlook Web App account locked for security reasons.

Thank you,  
Maintenance and Operations.

Source: Email Security Team.

Office 365





# AI PHISHING PROTECTION

Sender's name has brand-related text

Subject language often used for phishing

Sent to a senior recipient

Low traffic website

Suspicious body text language

+300 more email indicators

From: Josh Clair [mailto:josh365.clair@chu-miens365.fr]  
 To: Robert Hoffmier  
 Cc:  
 Subject: Email Security Team!

Your Microsoft Outlook Web Account has recently been subjected to security modification as of 12/18/2018. The action requested is as follows: This automated email contains a link to reset and maintain your Outlook Web App password as your current password has expired.

Please [Click Here](#) to go to the Reset Password page. Follow the instructions below to create a new password.

The link above expires after 24 Hours. If you do not change your password before then, your Outlook Web App account will be locked for security reasons.

Thank you,  
 Maintenance and Operations.

Source: Email Security Team.

ARTIFICIAL INTELLIGENCE

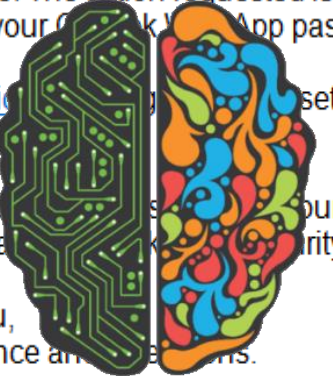
Convert **suspicious** into accurate **verdict**

Suspicious body text language

Verdict: PHISHING  
 Action: QUARANTINE

Sender's name has brand-related text

Sent to a senior recipient



A new generation of email threats...

## BUSINESS EMAIL COMPROMISE (BEC)



**\$26 billion lost in BEC scams in past 3 years**

Impersonate real user

Business context

Financial fraud

Purely textual

Call for action

# SandBlast AI blocks BEC fraud



Mon 07/10/2019 14:23

Gil Shwed <gshwed@us.checkpoint.com>

Verbraken Lawyer case

To [redacted]

VIP

Sense of Urgency

“high priority”

Good morning Ron,

I need you to manage a high priority operation with my Attorney Laurent Verbraken It's about a prime concern 1.16.1... corporation bid acquisition.

Secrecy

Verbraken associates lawyers offices asked me that do not treat this case from Headquarters and use a foreign subsidiary to avoid leaks and insiders trading. I will give you more information in next few hours. So, I did choose you to supervise this operation with my lawyer.

“No one else except us must be informed at this time”

No one else except us must be informed at this time. Regarding this case the Financial Markets Authority has warned us that we must communicate only by email until the public announcement is made in the next few weeks.

First of all Ron, send me immediately the available cash flow (bank statements) of our bank accounts in Canada. Also give me another phone number where you are comfortable to speak with him.

Financial related

“send me immediately the available cash flow (bank statements) of our bank account”

As soon as I receive those information, I will share with you further instructions for today.

Best regards,


Gil Shwed

Sent from my iPhone




# Educating users on the phishing we block


Reply Reply All Forward  
Tue 30-Jul-19 9:44 AM  
antiphishing@checkpoint.com  
Blocked Phishing attempt  
To John@corporate.org

 Check Point  
SOFTWARE TECHNOLOGIES LTD.

Check Point Anti-Phishing had just blocked the email below because we suspect it to be a phishing attempt. If you believe that this is a legitimate email, please click [this link](#) and the blocked email will be delivered to you.

 **Resembles a Salesforce email address.**  
Note the missing letter 'e'

From: Salesforce account <account@salsforce.com>  
To: John@corporate.org  
Cc:  
Subject: Your Salesforce password has expired

 **Salseforce logo on non-Salesforce email**

**Password Expired**

**Dear customer,** **Generic non-personalized greeting**

Your password for the Salesforce account [john@corporate.org](#) **The link points to a low-reputation web-site that impersonates Salesforce**  
For your account security, your current password will cease to work shortly.  
You are required to change your password using this [link](#)  
This is a system notification, not an email message and you can't reply to it.

Sincerely,  
The Salesforce Team

An image  
of a blocked email

# Some email attacks only manifest in the web session



First layer of security

Second layer of security

# Click-time inspection



From: Paypal  
To: Bruce Kornpique  
Cc:  
Subject: PayPal account verification

Message

Dear Paypal member,

Please sign in to <http://gw.example.com/?id=xghGGr92> to verify your PayPal account.

If you are using Internet Explorer please allow ActiveX for scripts to perform all data transfers securely.

Thank you for using PayPal !

*Rewrite URL before mail delivery*

*Link forced to go through cloud security*

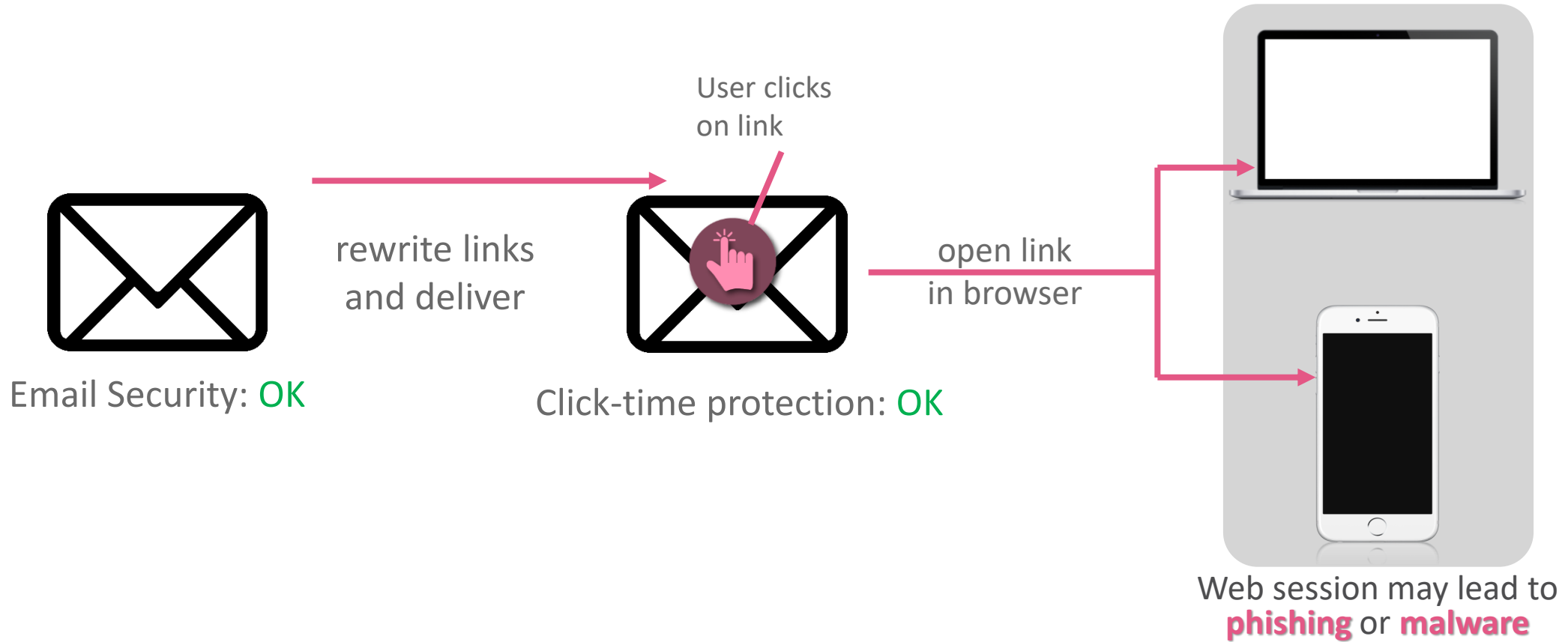
*Click-time link scanning – even if user is not behind a gateway*

Reputation

Threat Emulation

Threat Extraction

# Some email attacks only manifest in the web session



First layer of security

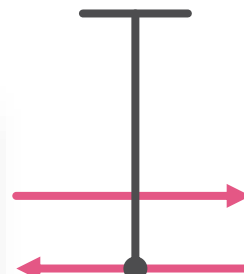
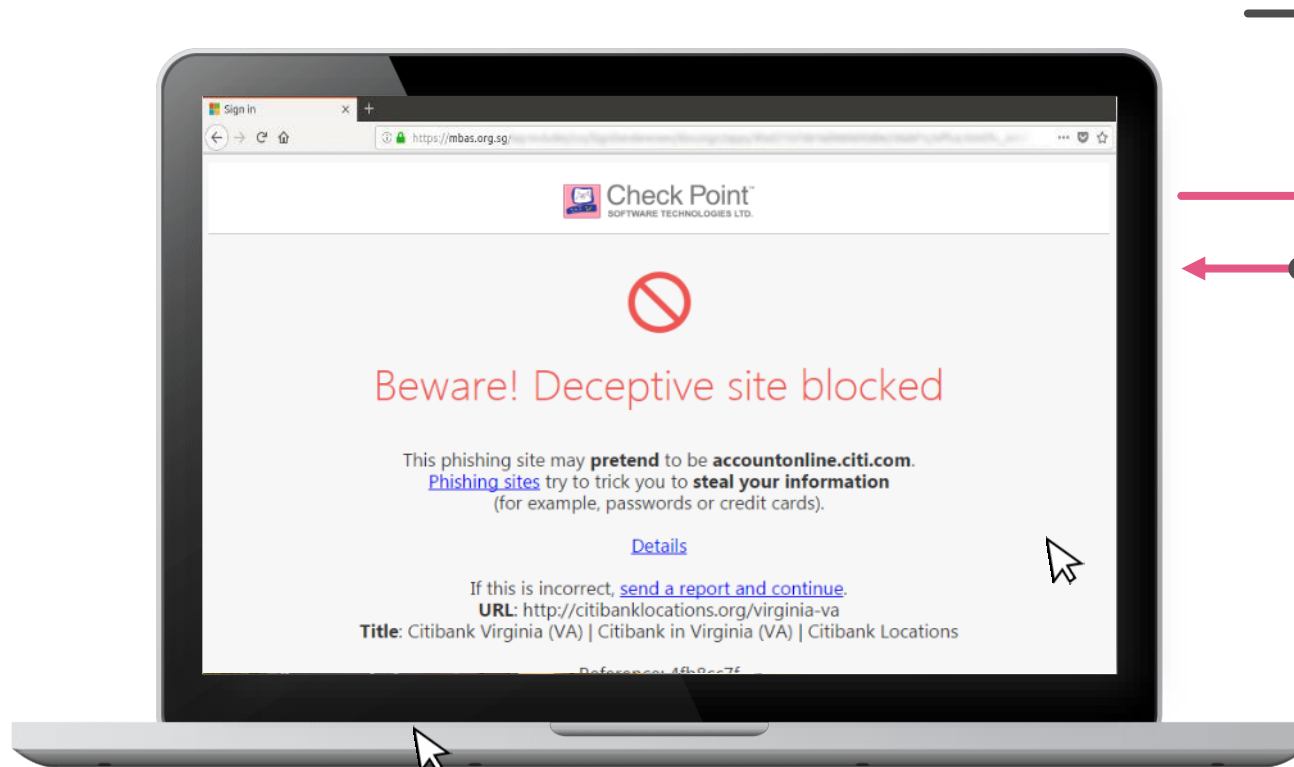
Second layer of security

Third layer of security



# Zero Phishing: prevent zero-day phishing in browser

Verdict: **Zero-day** phishing site



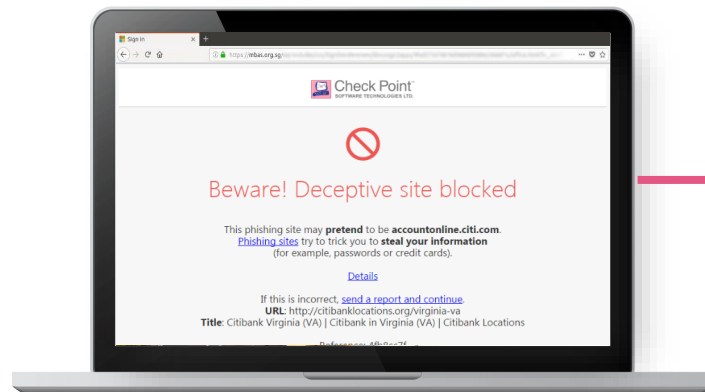
## THREATCLOUD

- ✓ IP Reputation
- ✓ Domain Reputation
- ✗ URL Similarity
- ✓ Lookalike Characters
- ✗ Title Similarity
- ✗ Image Only Site
- ✗ Visual Similarity
- ✗ Multiple Top-Level Domain
- ✗ Text Similarity
- ✗ Lookalike Favicon

+dozens more indicators

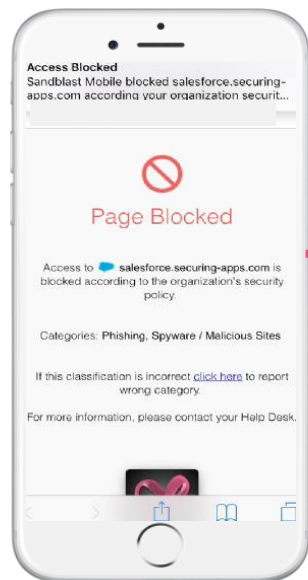
ZERO-DAY PHISHING SITE **PREVENTED!**

# Follows the user - web-session protection



ZERO-DAY PHISHING PREVENTION

ZERO-DAY MALWARE PREVENTION



ZERO-DAY PHISHING PREVENTION

MALICIOUS APP DOWNLOAD PREVENTION

# SandBlast 2020 – what's new?



**Fast  
Inline Prevention**



**Advanced  
Email Protection**

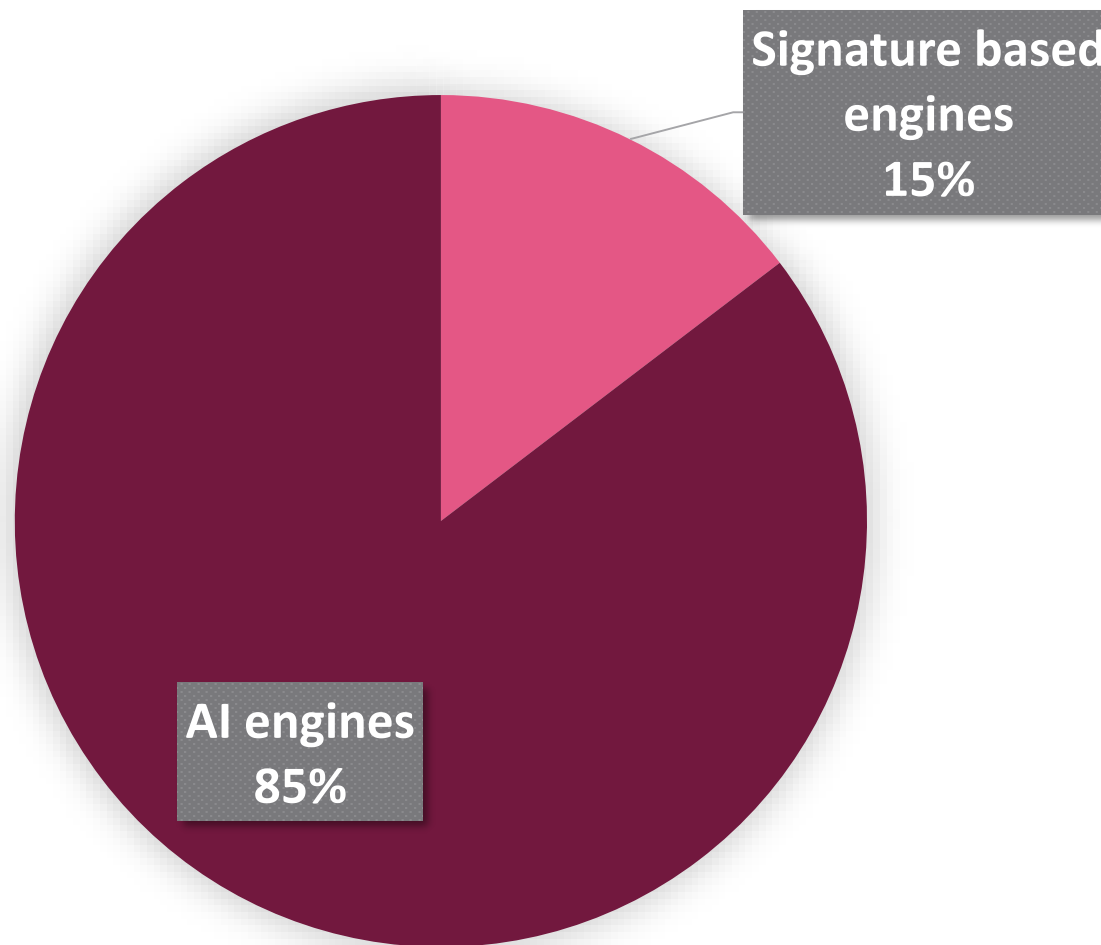


**Artificial  
Intelligence**

**The world's best zero-day prevention. Period.**

# Our detections in Q4-2019

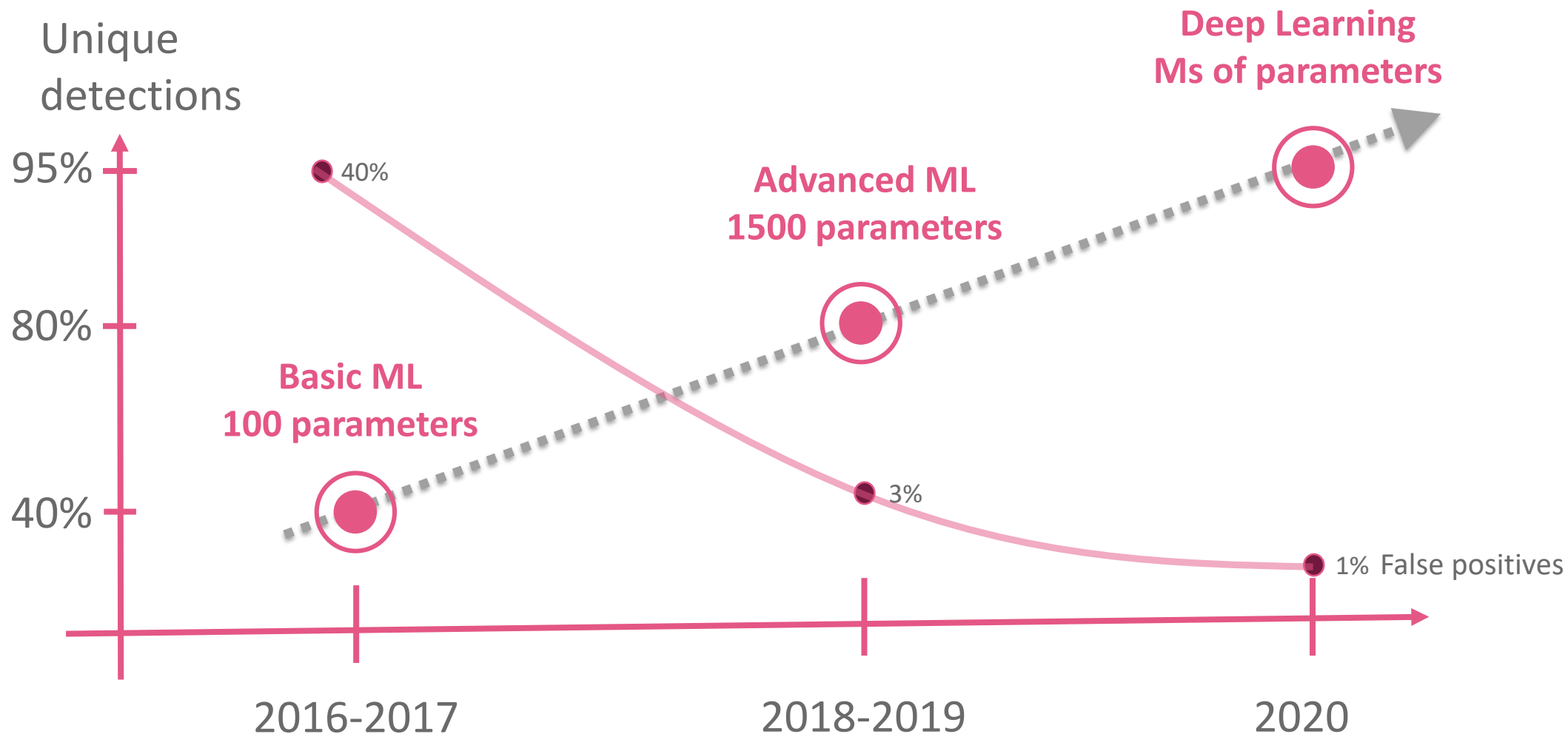
# AI







# Evolution of our Artificial Intelligence Engines



# What do we use AI for?



Detect unknown malware, accurately

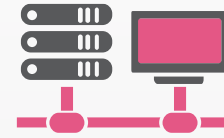
Classify unknown malware

Campaign hunting

Expose stealth breaches

Anomaly detection

Detect unknown phishing attacks



network



Cloud



Endpoint



Mobile



Email

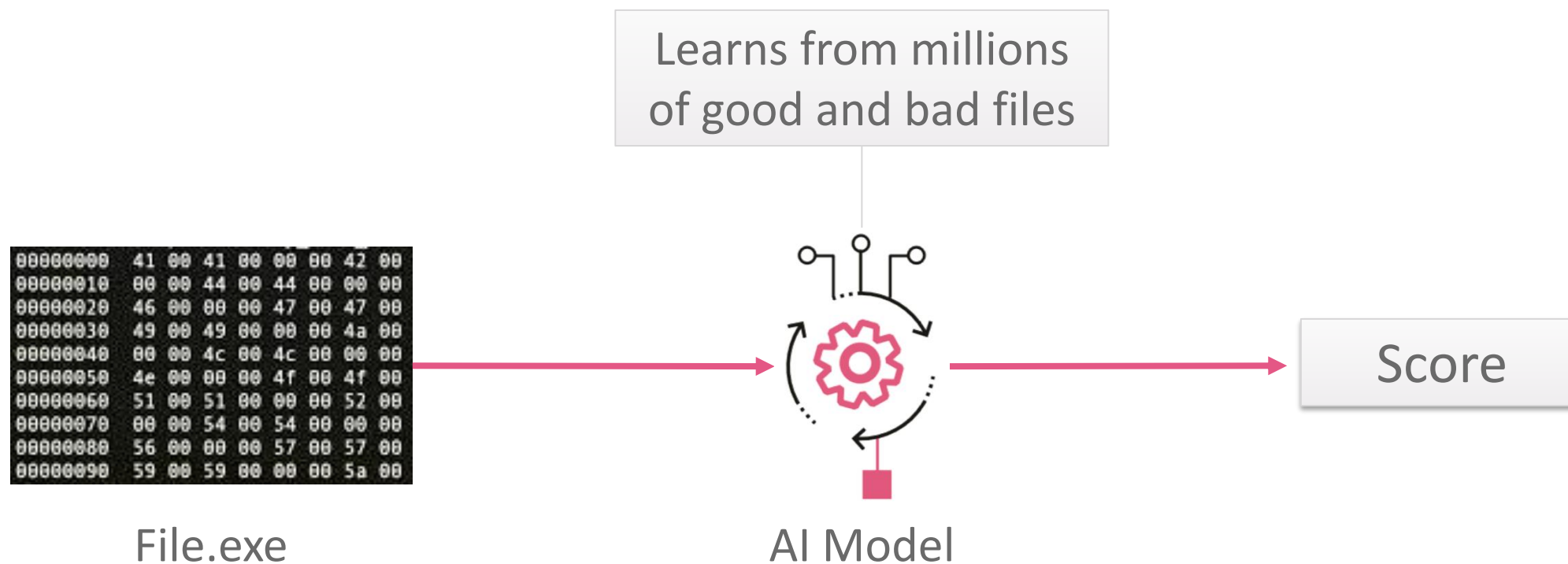


IoT



SECURITY

# Our first generation AI engines (2016)

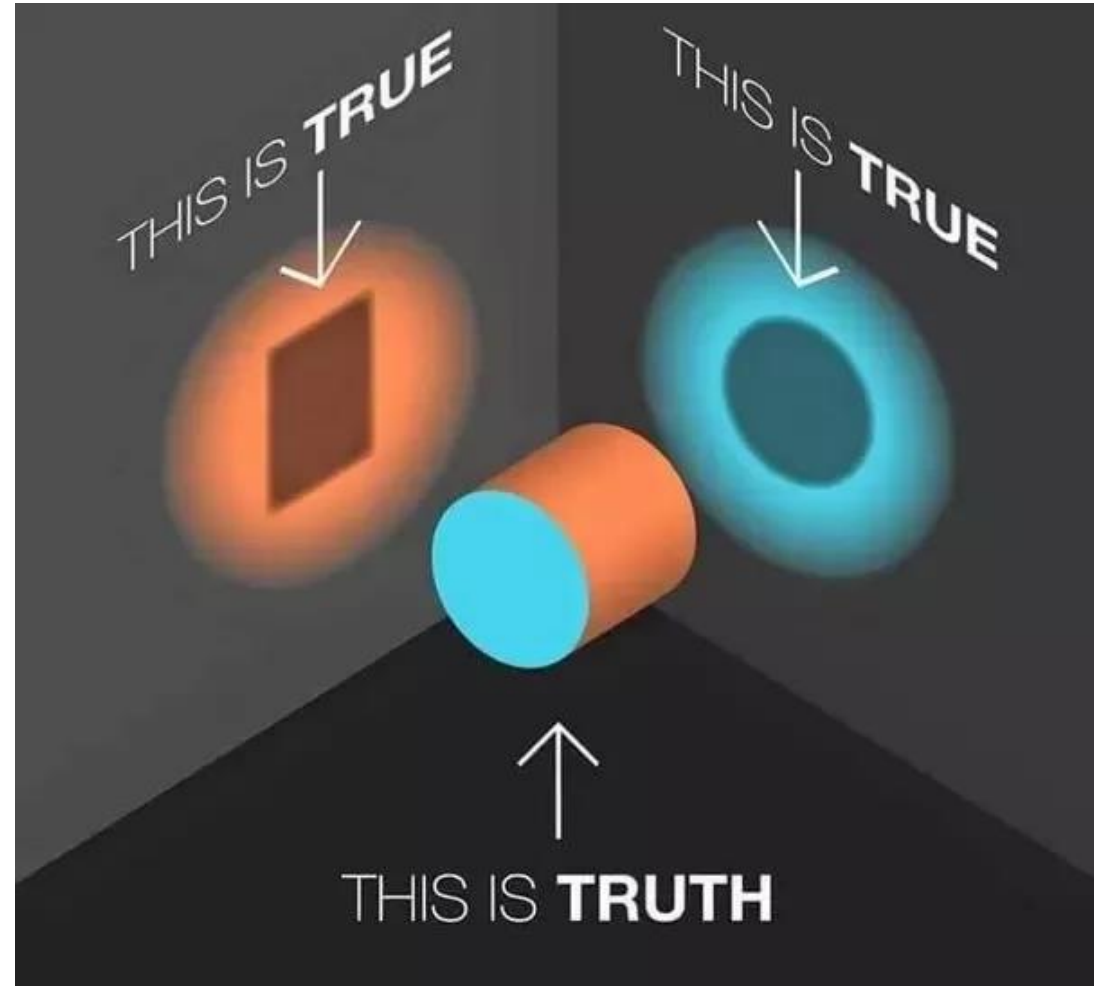


Supervised model  
100 parameters, expert selection

# How can we improve AI detection?



CHANGE OUR  
**PERSPECTIVE**





# New perspectives on a binary files



file = stream of bytes

00000000	41 00 41 00 00 00 42 00
00000010	00 00 44 00 44 00 00 00
00000020	46 00 00 00 47 00 47 00
00000030	49 00 49 00 00 00 4a 00
00000040	00 00 4c 00 4c 00 00 00
00000050	4e 00 00 00 4f 00 4f 00
00000060	51 00 51 00 00 00 52 00
00000070	00 00 54 00 54 00 00 00
00000080	56 00 00 00 57 00 57 00
00000090	59 00 59 00 00 00 5a 00

file.exe

convert

## Textual representation

```
ccessId GetModuleHandle QueryInformationProcess GetModuleHandle GetProcAddress Q  
me GetFileAttributes FindFirstFile GetFileAttributes GetModuleHandle GetProcAddr  
de QueryInformationProcess LdrLoadDll CreateFile CreateProcess LdrLoadDll Create  
ess FindFirstFile CreateFile ReadFile SetLastError QueryInformationProcess Unmap  
WaitForSingleObject LoadLibrary LdrLoadDll CreateFile GetProcAddress RegCloseKe  
GetProcAddress RegCloseKey FindFirstFile RegCloseKey LdrLoadDll CreateFile Query  
ProcAddress GetModuleFileName QueryInformationProcess GetModuleHandle QueryInfor  
l CreateFile GetProcAddress RegCloseKey GetProcAddress GetModuleFileName GetFile  
reateFile CloseHandle LdrLoadDll CreateFile GetProcAddress CreateFile RegCloseKe  
OfFile QueryInformationProcess CloseHandle UnmapViewOfFile UnmapViewOfSection CL  
MapViewOfFile QueryInformationProcess CloseHandle UnmapViewOfFile UnmapViewOfSe  
ll CreateFile GetProcAddress RegCloseKey CreateFile CloseHandle LdrLoadDll Creat  
eHandle GetProcAddress QueryInformationProcess GetCurrentThread QueryInformation  
QueryInformationProcess RegCloseKey QueryInformationProcess GetModuleFileName L  
tErrorMode QueryInformationProcess LdrLoadDll CreateFile GetProcAddress CreateFil  
e GetProcAddress GetCurrentProcess QueryInformationProcess GetProcAddress GetCur  
address GetModuleFileName GetCurrentProcess QueryInformationProcess GetModuleFile  
ModuleHandle GetProcAddress RegCloseKey GetCurrentProcessId GetModuleHandle GetP  
cess GetProcAddress CloseHandle GetProcAddress GetCurrentProcessId CreateFileMan
```

File.txt

## Image representation



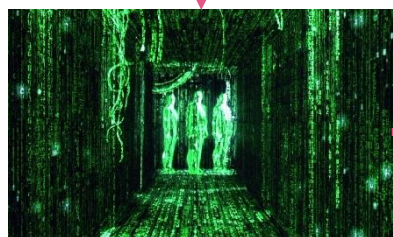
File.jpg



# Adding new AI perspectives

## Textual Representation

```
processID GetModuleHandle QueryInformationProcess GetModuleHandle GetProcAddress  
GetFileAttributes FindFirstFile GetFileAttributes GetModuleHandle GetProcedu  
r QueryInformationProcess LdrLoadDll CreateFile CreateProcess LdrLoadDll Creat  
ess FindFirstFile CreateFile ReadFile SetLastError QueryInformationProcess Unmap  
WaitForSingleObject LoadLibrary LdrLoadDll CreateFile GetProcAddress RegCloseKe  
GetProcAddress RegCloseKey FindFirstFile RegCloseKey LdrLoadDll CreateFile Query  
ProcAddress GetModuleFileName QueryInformationProcess GetModuleHandle QueryInfor  
mationProcess CreateFile GetProcAddress RegCloseKey GetProcAddress GetModuleFile  
CreateFile CloseHandle LdrLoadDll CreateFile GetProcAddress CreateFile RegCloseKe  
y QueryInformationProcess CloseHandle UnmapViewOfFile UnmapViewOfFile CT  
hreadViewOfFile QueryInformationProcess CloseHandle UnmapViewOfFile UnmapViewOfSe  
ct CreateFile GetProcAddress RegCloseKey CreateFile CloseHandle LdrLoadDll Creat  
eFile GetProcAddress QueryInformationProcess GetCurrentThread QueryInformation  
QueryInformationProcess RegCloseKey QueryInformationProcess GetModuleFileName L  
drLoadDll QueryInformationProcess LdrLoadDll CreateFile GetProcAddress CreateFil  
e GetProcAddress GetCurrentProcess QueryInformationProcess GetProcAddress GetCur  
rentProcess GetCurrentProcess QueryInformationProcess GetModuleFile  
ModuleHandle GetProcAddress RegCloseKey GetCurrentProcessID GetModuleHandle Get  
ProcAddress CloseHandle GetProcAddress GetCurrentProcessID CreateFile
```



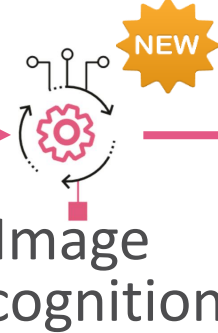
## Image Representation



Score



Score

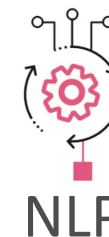


Score

# Adding new AI perspectives

We have **dozens of verdicts**  
for each file.

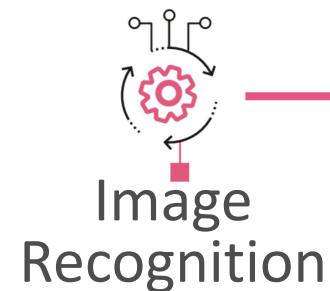
So, **how do we decide?**



Score

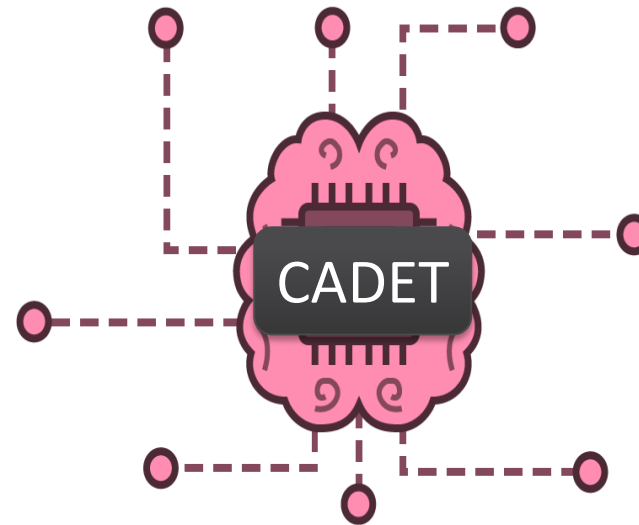


Score



Score

# CADET: The ML of MLs

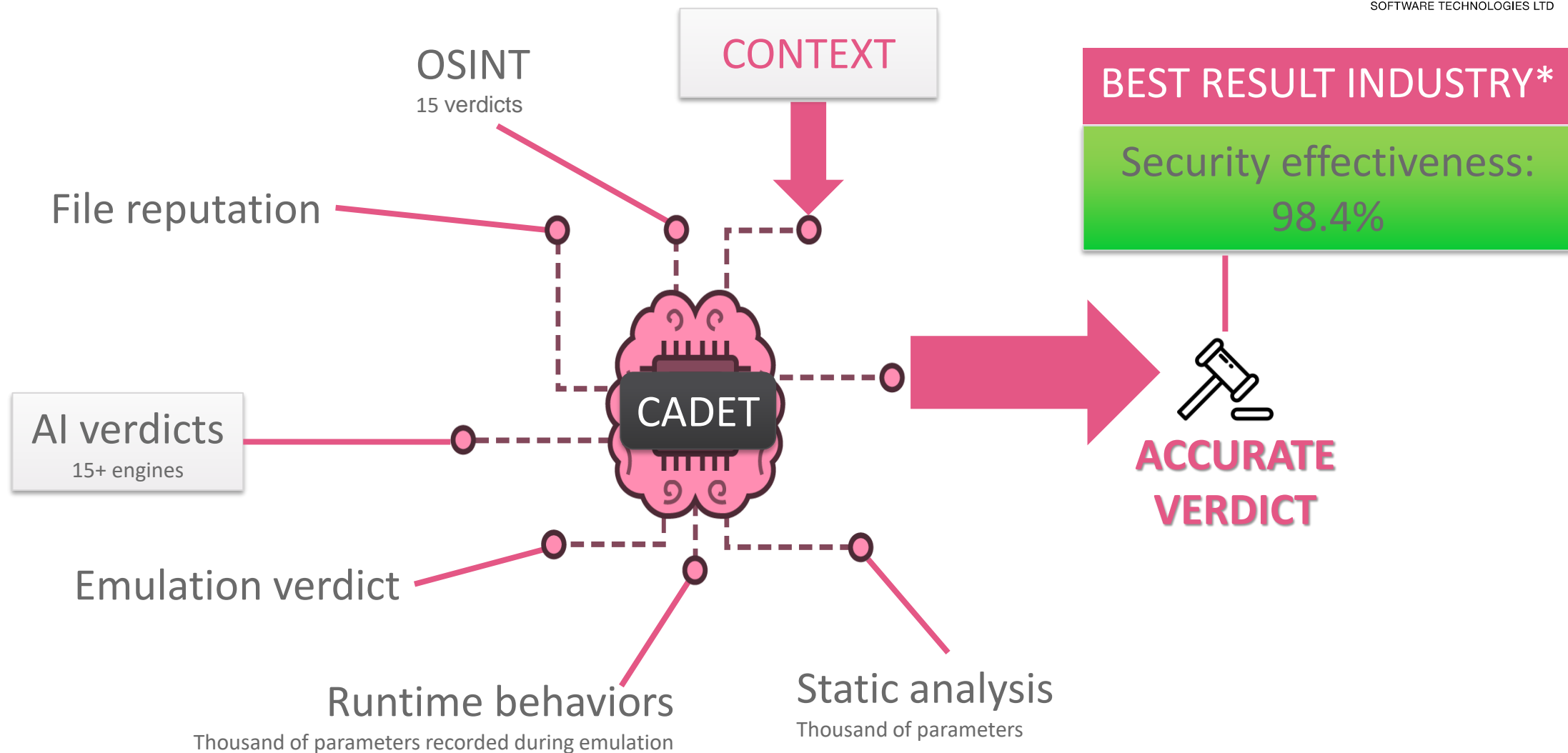


## CADET - Context Aware Detection





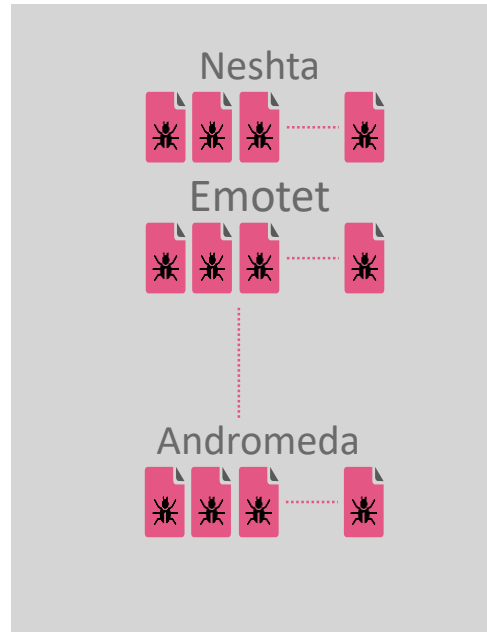
# CADET: The ML of MLs



\* NSS BPS test result, 2019

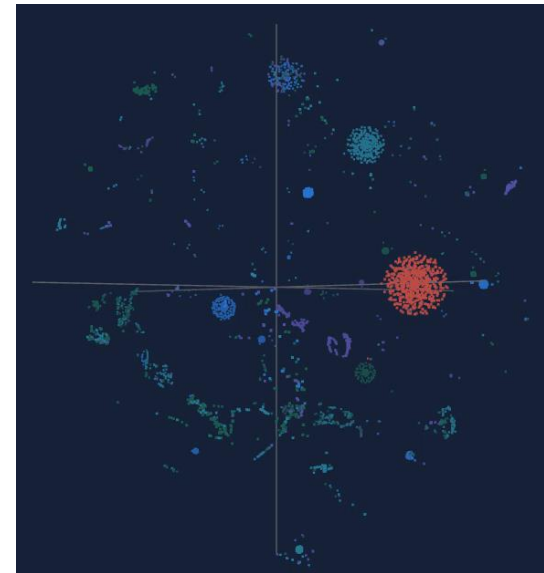
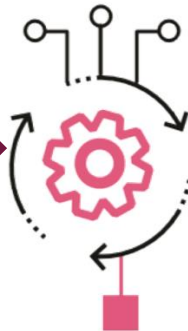
# Unknown Malware Classification

## Multidimensional model



Malware Families

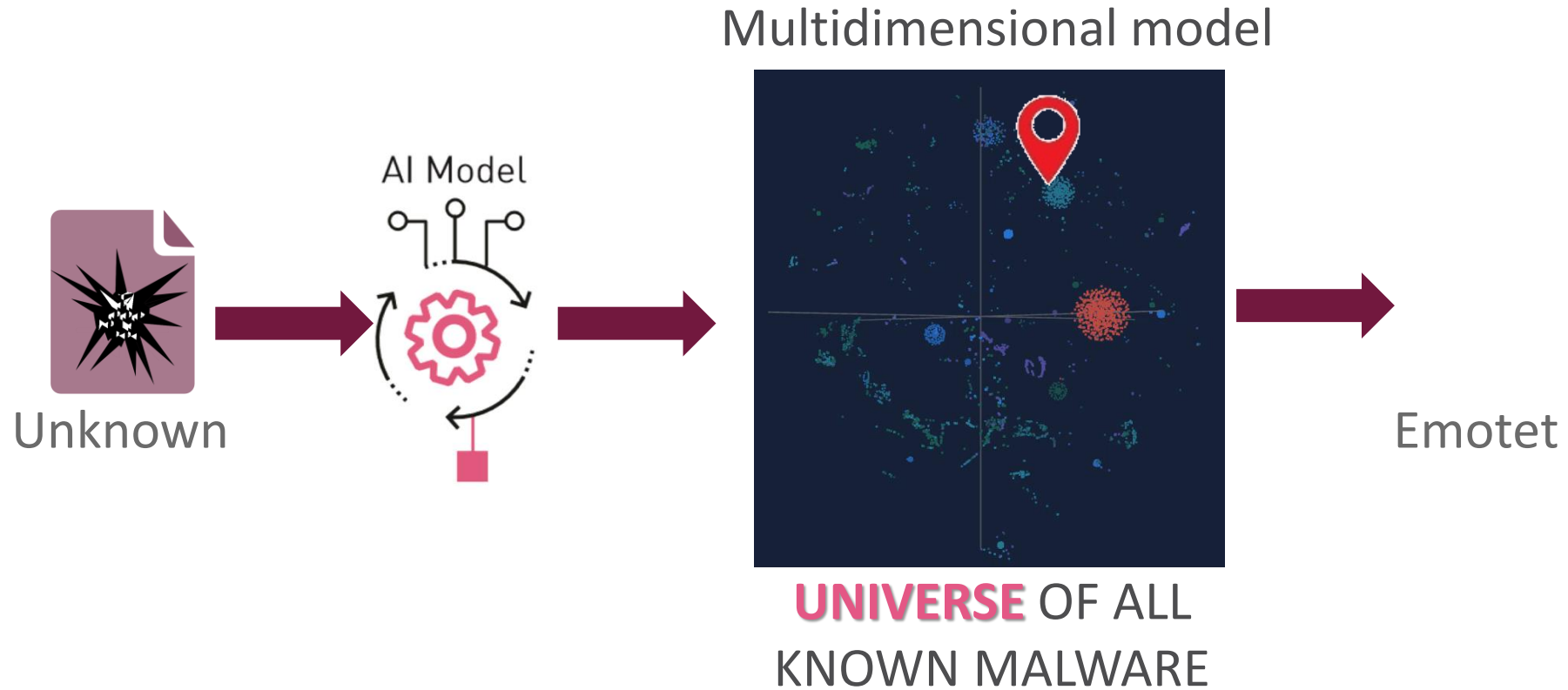
AI Model



**UNIVERSE** OF ALL  
KNOWN MALWARE

Each galaxy represents all known permutations of a malware family members

# UNKNOWN MALWARE CLASSIFICATION



**Over 98% classification accuracy**

# SandBlast 2020 – what's new?



**Fast  
Inline Prevention**



**Advanced  
Email Protection**



**Artificial  
Intelligence**

The world's best zero-day prevention. Period.



# Our time's up, but there's lots more coming...





LET'S SUMMARIZE



# FOR A BETTER 2020



**Fast  
Inline Prevention**



**Advanced  
Email Protection**



**Artificial  
Intelligence**

**PREVENT ZERO-DAY ATTACKS WITH SANDBLAST**

# Thank you!

## WHAT NEXT?

Visit us in the  
tech room

Activate SandBlast  
in your network



# SUBSCRIBE TO

# cp<r>radio>

CHECK POINT RESEARCH PODCASTS

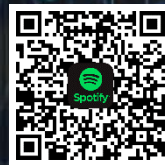
Listen on  
**Google Podcasts**



Listen on  
**Apple Podcasts**



Listen on  
**Spotify**



KEEP UP WITH THE LATEST CYBER SECURITY RESEARCH

[research.checkpoint.com](https://research.checkpoint.com)