Top Threats to Watch Out for in 2019

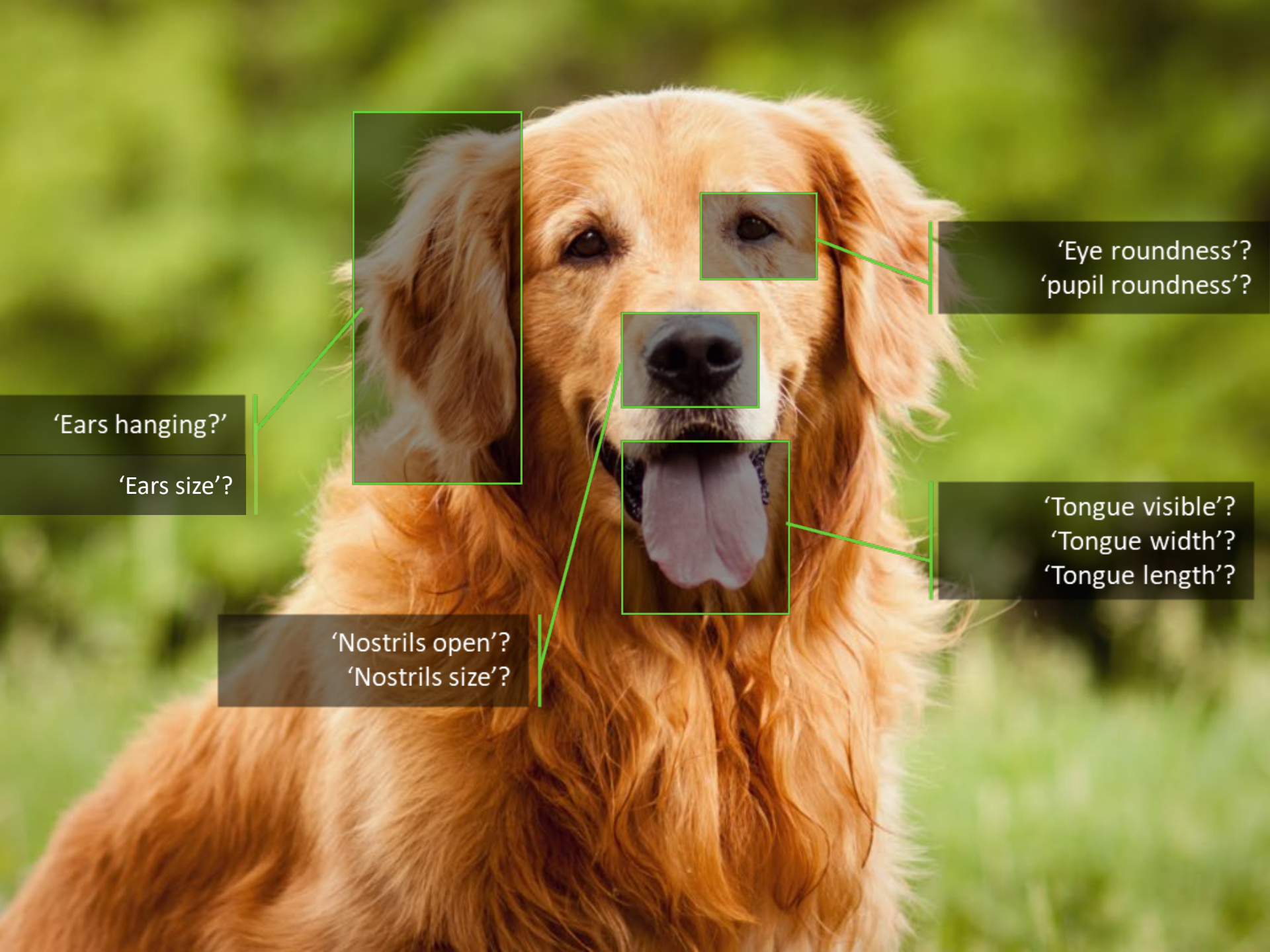
How AI Can Help Protect Against Them

Himanshu Verma
Director, Global Business Development

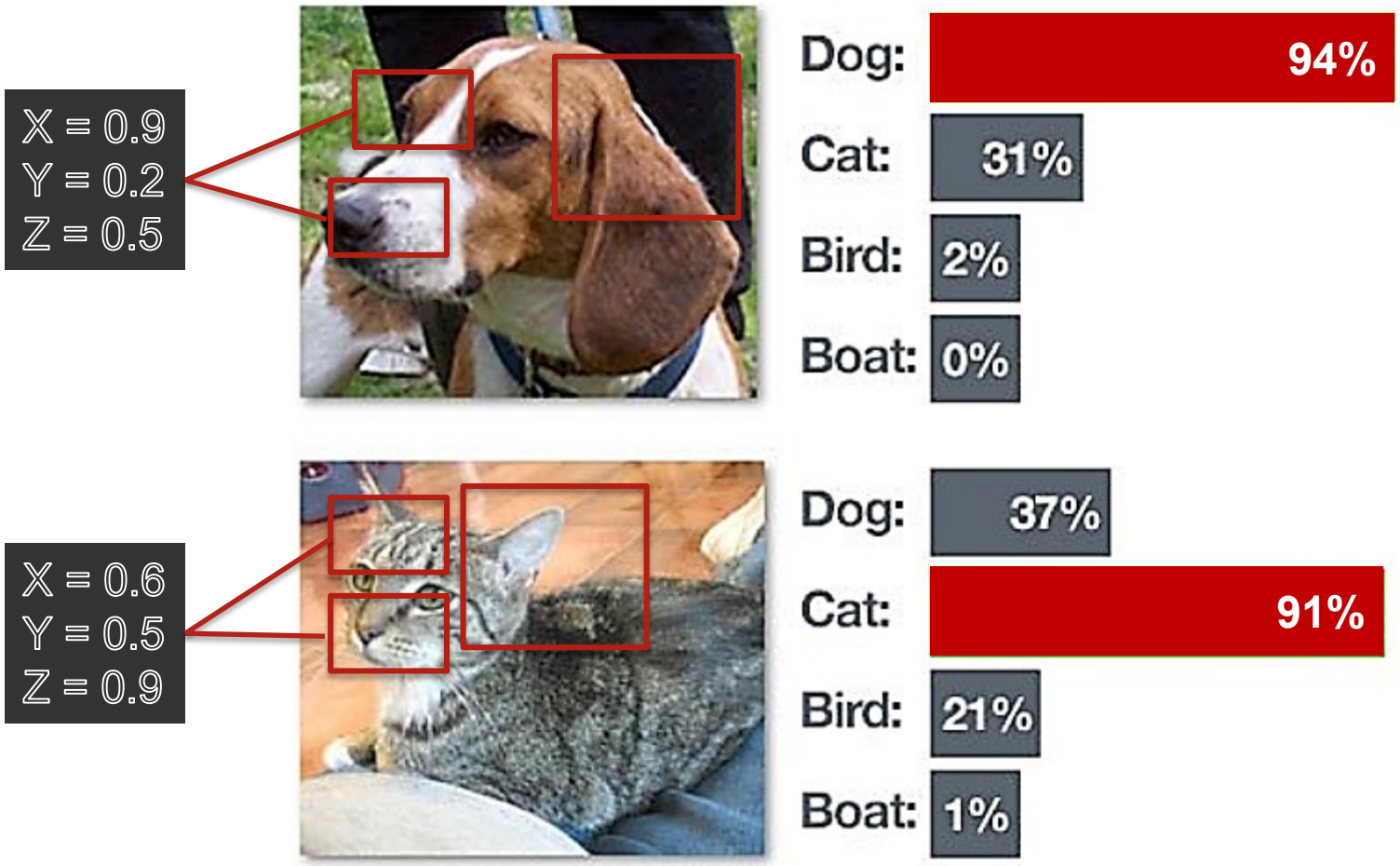
Artificial intelligence

(noun)

1 :a branch of computer science dealing with the simulation of intelligent behavior in computers.
2 :the capability of a machine to imitate intelligent human behavior.

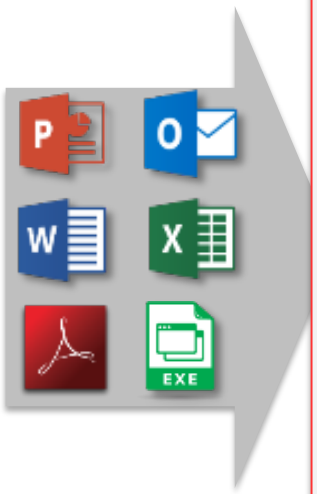

‘Ears hanging?’
‘Ears size’?
‘Eye roundness’?
‘pupil roundness’?
‘Nostrils open’?
‘Nostrils size’?
‘Tongue visible’?
‘Tongue width’?
‘Tongue length’?

Feature Classification



Artificial Intelligence Malware Identification

Whereas a human malware reverser might look at 10, 20 or 50 file characteristics to determine if a file is bad, Machine Learning (ML) can consider 1000's and 100K's of features all at once



DOS Header
NT Header
File Header
Section Headers
Export Directory
Import Directory
Resource Directory
Relocation Directory
Debug Directory
Packer Used
Compiler Type
Compiler Language
File size
PE size
Image section headers
Functions called
Kernel hooks
Image Paths
Image Resource Directory
Bitmaps
Icons
Strings
RCData
Version Info…


```
lea     rcx,[rdi+20h]
mov     qword ptr [rdi+10h],r13
lea      rdx,[rsp+258h]
or       r9,0FFFFFFFFFFFFFFFFh
xor      r8d,r8d
mov     word ptr [rcx+8],r13w
mov     ebx,r14d
```

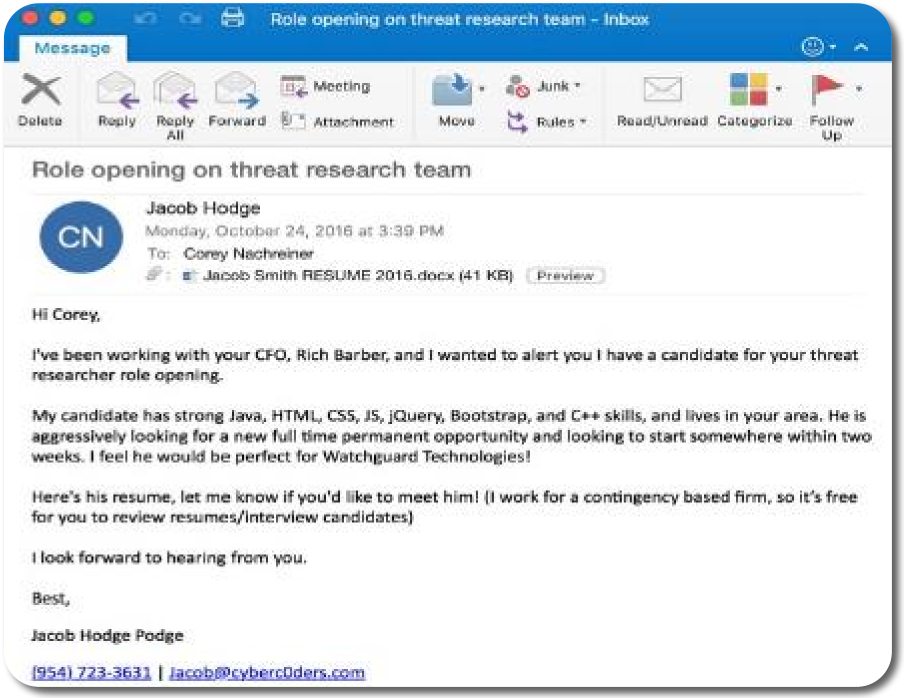
Spear-Phishing the Norm

Flavors of Phishing

Phishing – luring a victim into giving up credentials or doing something via a legitimate seeming email

Spear-phishing – A more customized phishing email that targets a specific individual or group

Whaling – spear-phishing that targets C-levels



Old phishing example:
- Not localized
- Bulk recipients
- Uses stale assets
- Malicious document

Spear-phishing example:
- Personalized to me
- Fits my job role
- Understands business relationships
- Sender makes sense in context
- Malicious attachment fits context

Prevention: DNS Blocking & Awareness Training

DNSWatch Filtering

Exhibit 2: Sample DNS Filtering Process

Focus on phishing Training


Ransomworms

What is a RansomWORM?

Ransomware is a form of malware that encrypts your files and demands you pay a ransom.

A **Worm** is a type malware that spreads automatically over your network.

A **Ransomworm** is extremely nasty ransomware that spreads to many computers in your network

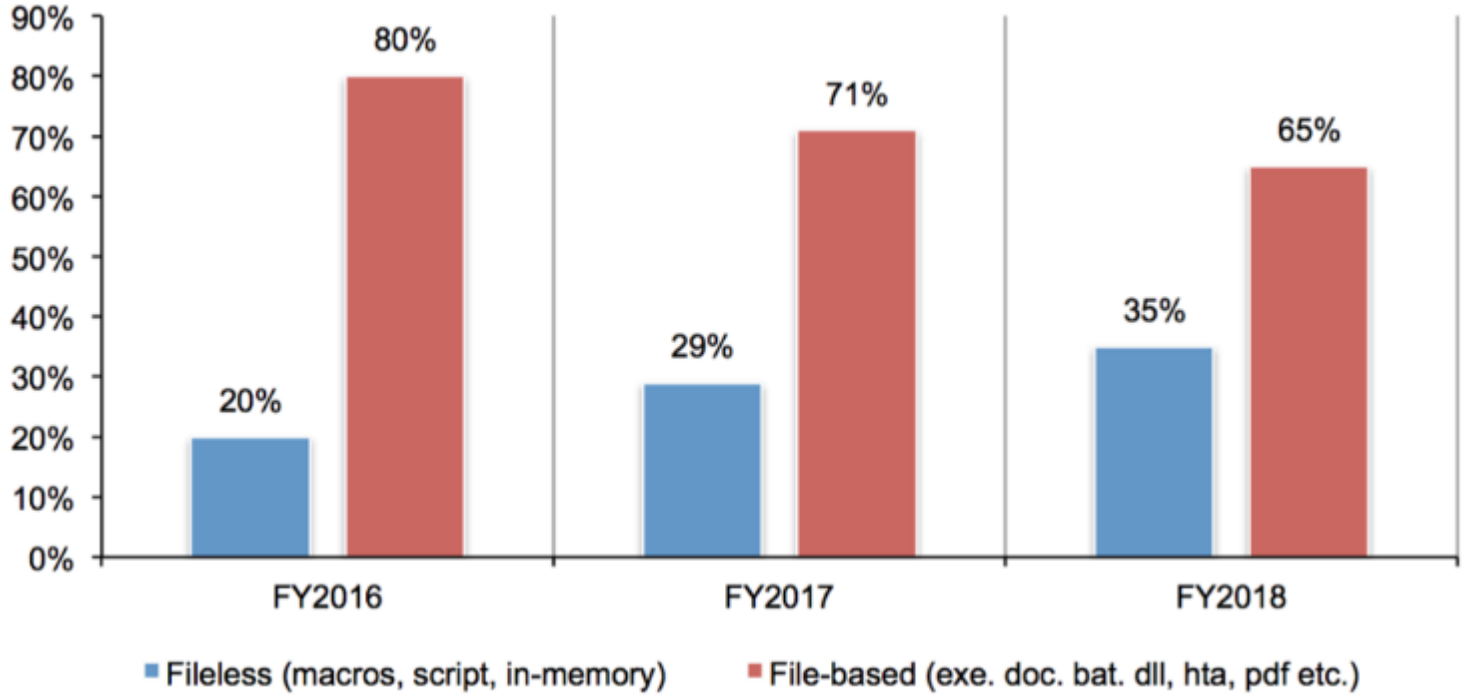
Prevention: Advanced Malware Detection

- Virtualizes a full victim system
- Runs unknown content in protected environment
- Analyzes behaviors
- Detects sandbox evasion
- Tracks additional malware and C&Cs

Fileless Malware

Fileless Malware Growing

Figure 2. The growth of fileless and file-based attacks



- 77% of attacks that successfully compromised organizations in 2017 utilized fileless techniques - *Ponemon Institute*
- Fileless malware attacks accounted for 52% of all attacks in 2017 - *Carbon Black*

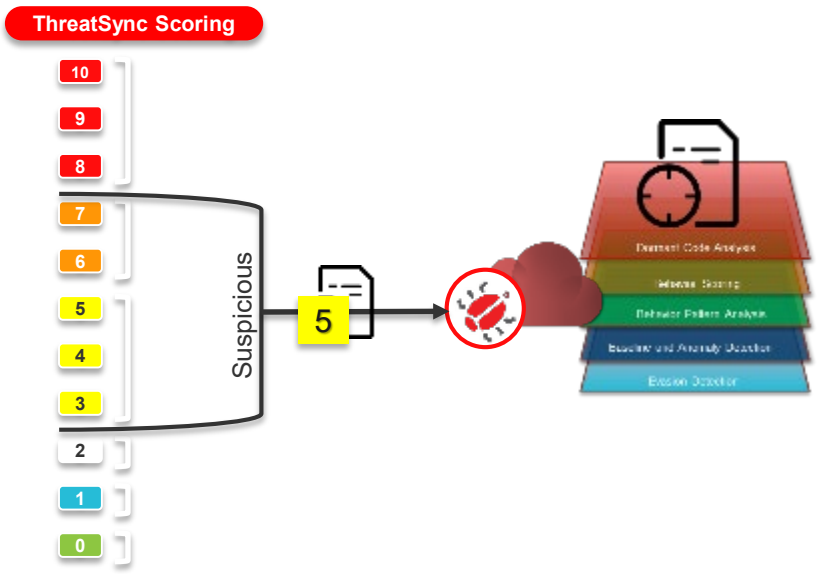
** Ponemon Institute's "The 2017 State of Endpoint Security Risk Report"*

Prevention: Detection and Response

- ThreatSync TI identifies known malicious processes
- Dynamic process heuristics finds suspicious processes
- HRP behavior detection could help too

Prevention: Detection and Response

ThreatSync uses AI in conjunction with APT Blocker to facilitate threat triage and automate threat defense.



1. With a foundation of AI, ThreatSync is regularly trained on thousands of malicious and benign files.

2. ThreatSync is able to automate the classification of suspicious files, and determine which should be sent to APT Blocker

3. APT Blocker will automatically return results to ThreatSync for automated remediation

WatchGuard Advances UTM with AI

What Value Does AI Bring to the WatchGuard Portfolio?

Predictive Protection

- The delay between when a malware strain is discovered, and when the signatures, heuristics, and behavioral patterns can be applied presents a significant challenge.
- IntelligentAV provides predictive coverage against malware threats an average of 25 months before they are seen in the wild

Shortened Time-to-Detect

- Detecting and killing highly evasive malware strains in a timely manner requires the knowledge and ability to look for thousands of malicious indicators.
- ThreatSync's in conjunction with our APT Blocker security service to detect and automatically send suspicious files for deep analysis in a next-generation Cloud sandbox.
- APT Blocker leverages AI during the deep inspection process to perform comprehensive analysis on files

Automated Threat Defense

- Artificial intelligence makes it possible to collect vast amounts of data from nearly every source imaginable and use that data to automatically train for secure outcomes.
- IntelligentAV, APT Blocker, and ThreatSync are constantly evolving from a steady stream of new data and feedback and applying this training to improve security posture.

Total Security Suite: with AI built-in, at 3 levels

The "predictive advantage" is the ability of ML models in TSS to prevent tomorrow's malware with today's machine learning models

Features & Services	TOTAL SECURITY SUITE	Basic Security Suite
Intrusion Prevention Service (IPS)	✓	✓
App Control	✓	✓
WebBlocker	✓	✓
spamBlocker	✓	✓
Gateway AntiVirus	✓	✓
Reputation Enabled Defense (RED)	✓	✓
Network Discovery	✓	✓
APT Blocker	✓	
Data Loss Protection (DLP)	✓	
Threat Detection & Response	✓	
DNSWatch	✓	
Access Portal*	✓	
IntelligentAV*	✓	
Dimension Command	✓	
Support	Gold (24x7)	Standard (24x7)

*Available on Firebox M Series appliances