FortiGuard AI

Smart Cyber Security

Simon Bryden, Consulting SE

SECURITYDAY

v1

What is FortiGuard?

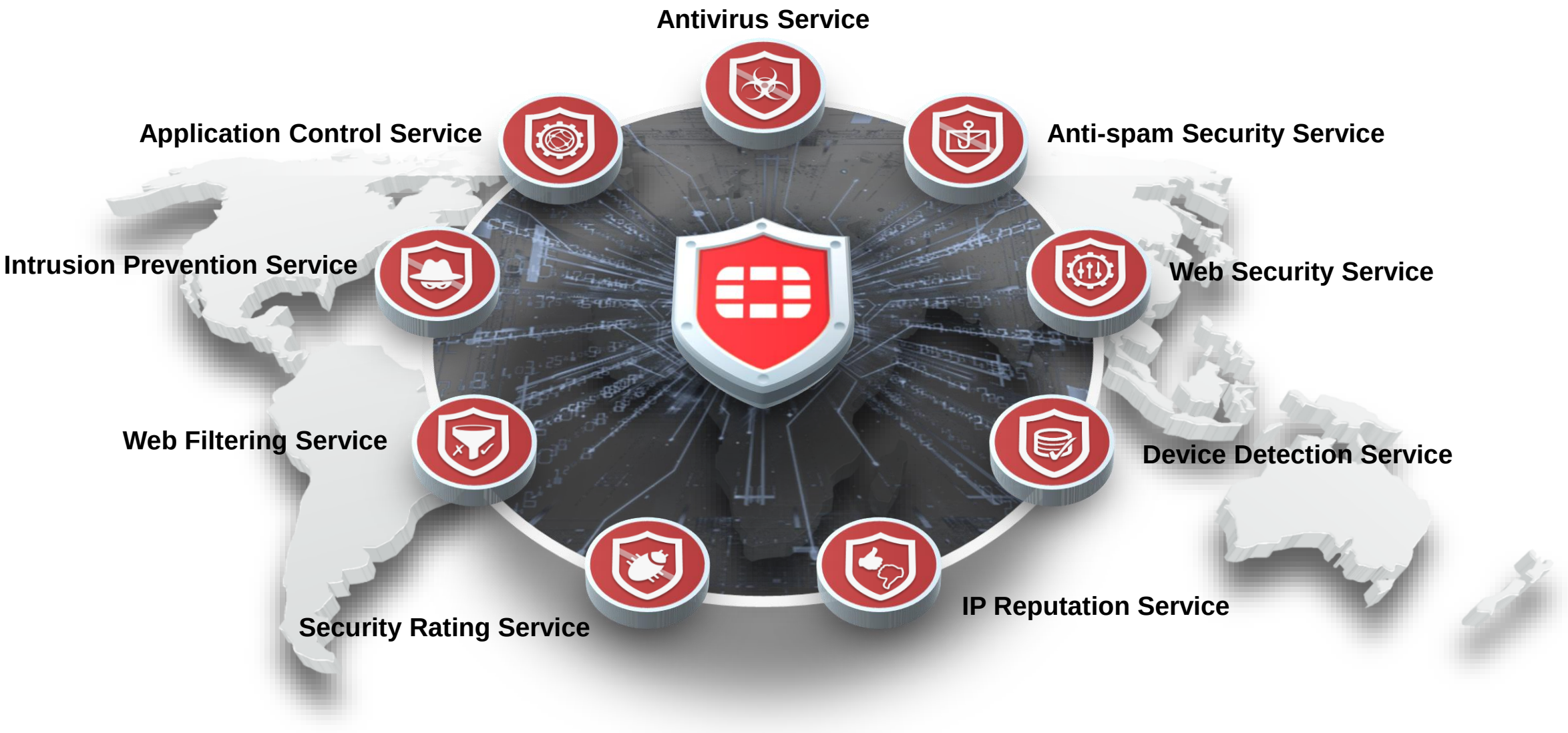
Fortinet Threat Research
- Malware and URL analysis
- Analysis of current threats
- Finding unknown vulnerabilities

Development
- Antivirus Engine
- Intrusion Prevention Engine
- Signature development

Innovation
- Automation of analyst tasks
- Leveraging emerging technologies

Customer Service
- Signature creation
- URL categorisation
- Premier services

FortiGuard Services



FortiGuard By The Numbers

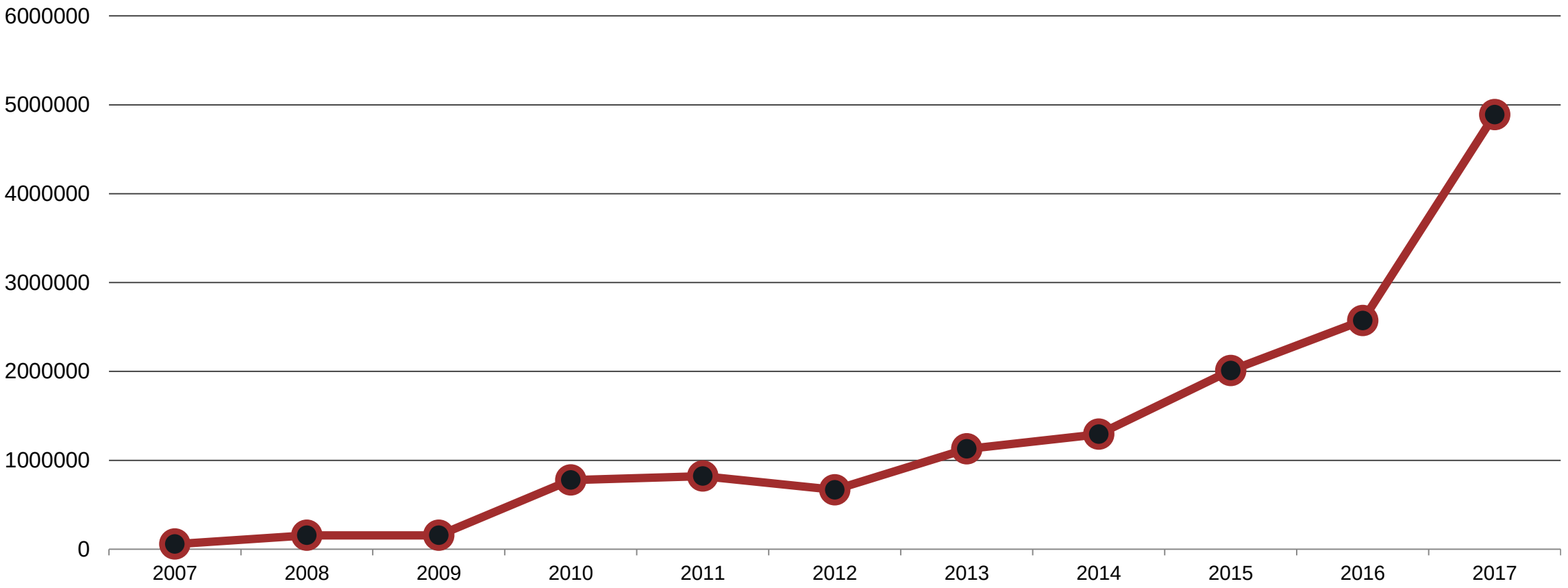
Strength

- 18 years of protection
- 200+ in Security Operations
- Extensive IT infrastructure
- 130+ Global Distribution Servers
- 360,000+ Customers

Threat Protection Challenges

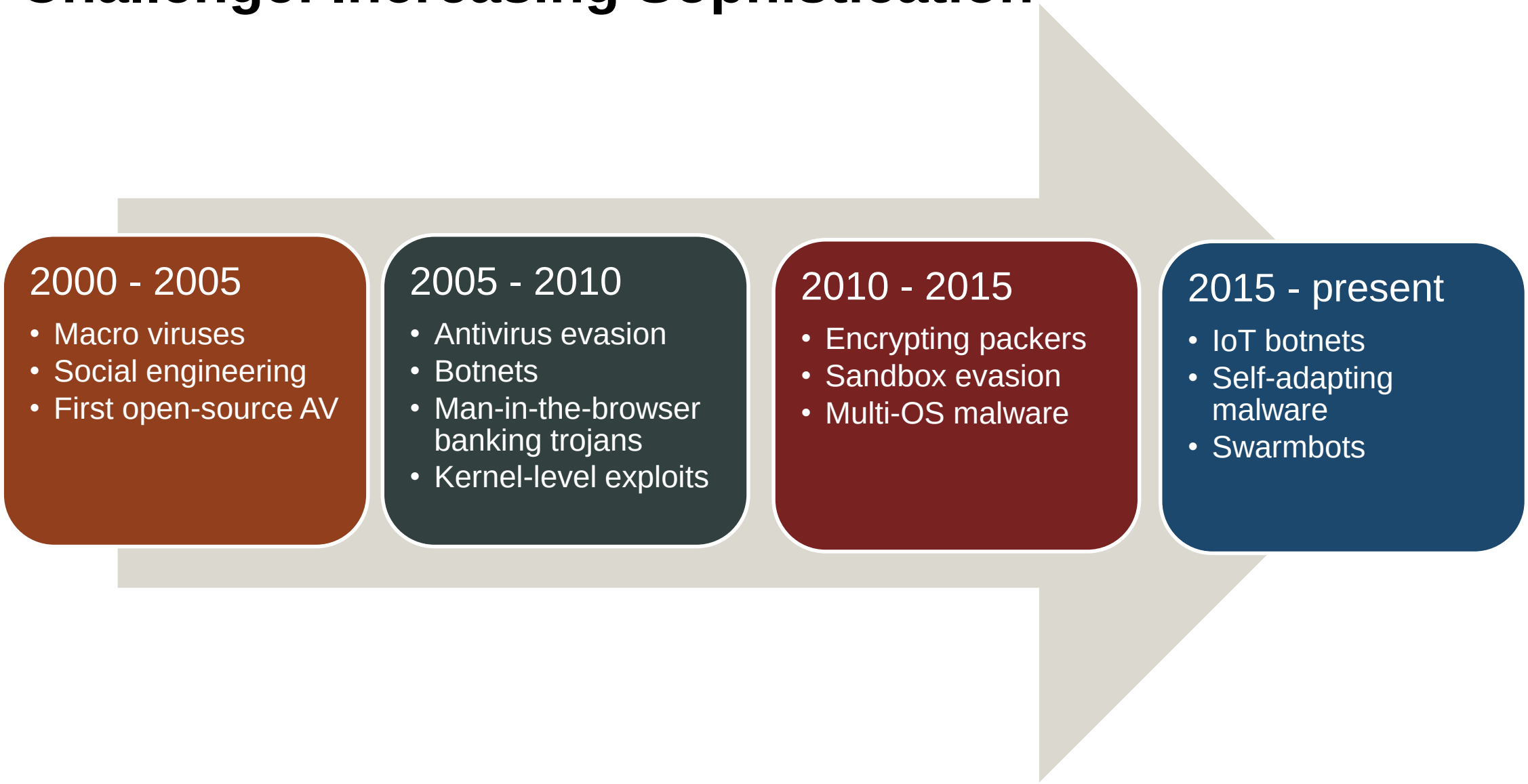
Challenge: Rising Volume

New malware from all sources per week



Source: FortiGuard Labs

Challenge: Increasing Sophistication



Challenge: Growing Attack Surface





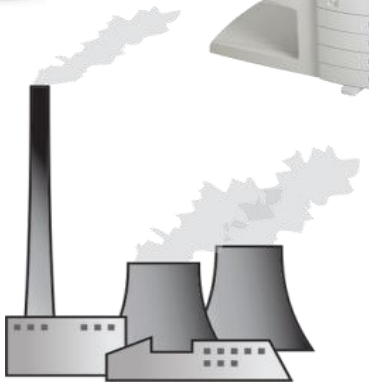










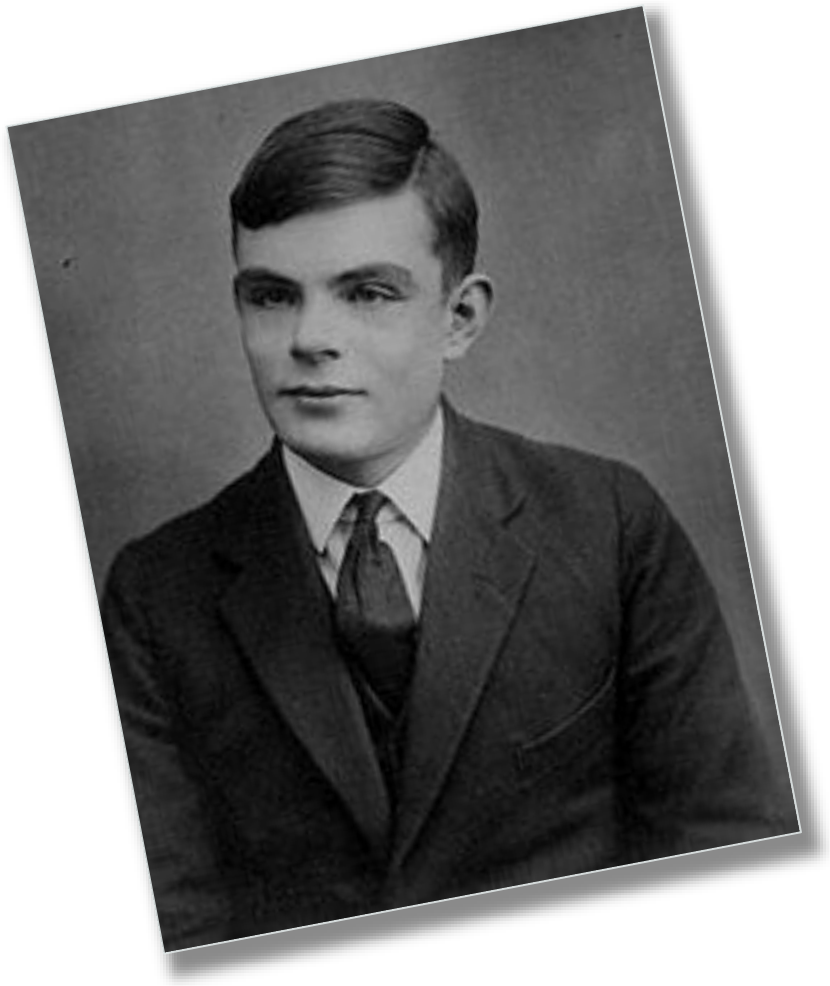


FORTINET

An Introduction to Machine Learning

SECURITYDAY

Early AI Defined



ALAN TURING
CALLED AN INFANT'S MIND AN 'UNORGANIZED MACHINE' IN 1930s

Created early definitions of machine learning

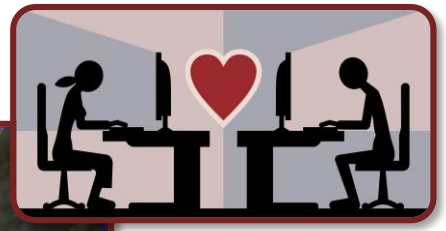
Major inhibitor of his research – his ideas were way ahead of available computing capabilities

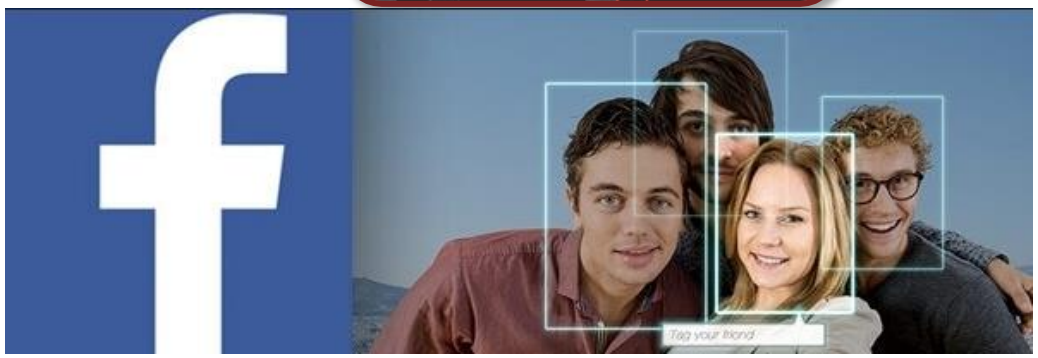
Part of Everyday life

Google

Spotify®

NETFLIX





amazon

Machine Learning Types

Supervised	Train using known labeled data E.g. optical character recognition
Unsupervised	Establish a baseline. Look for anomalies E.g. Suspicious behavior detection
Reinforcement	Make decisions to maximize reward E.g. game playing

Supervised Learning

Unsupervised Learning

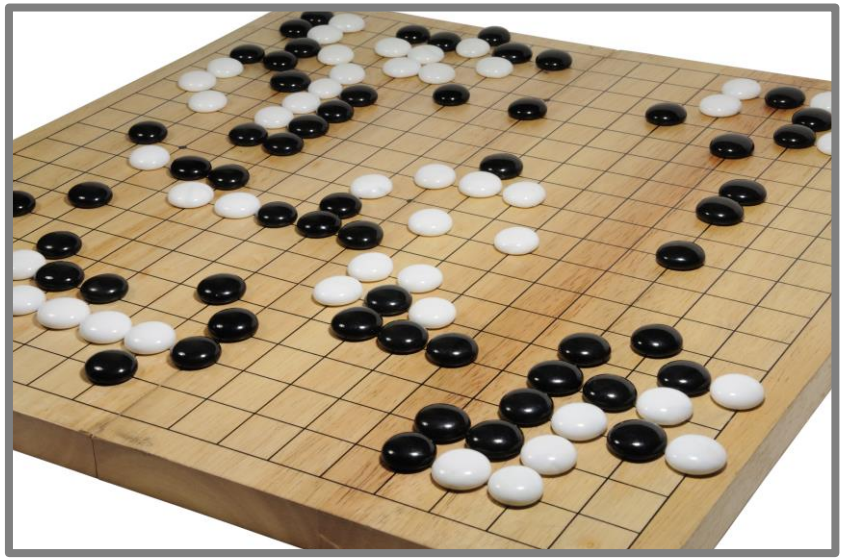
- Establish a baseline behavior
  - » Types of purchase
  - » Amounts of purchase
  - » Geographical distribution
- Trigger when transactions don’t match baseline

Reinforcement Learning

- From a given position, try a move based on current knowledge
- If resulting game won, increase weight for all moves in the game
- If game lost, decrease weight

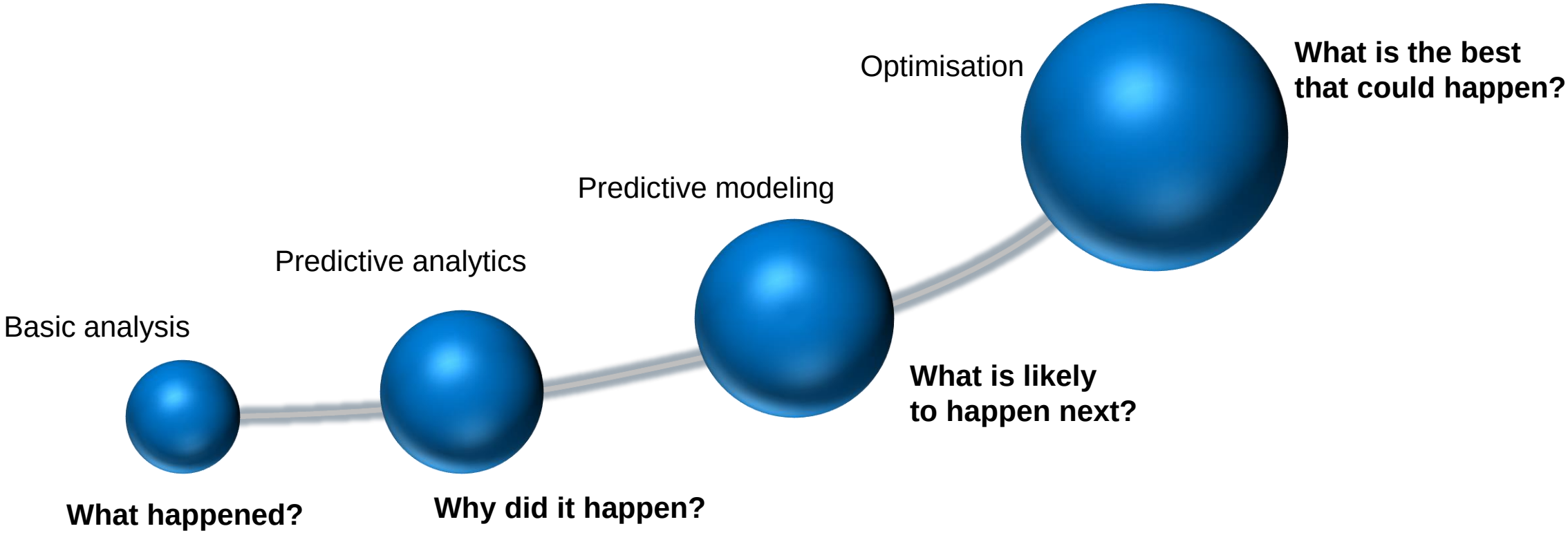
AlphaGo

- AlphaGo was Go playing machine
- Created by DeepMind, later acquired by Google
- Based on dual neural networks
- Trained with historical human matches
- Was able to beat Lee Sedol, 9-dan professional in 2016
- Went on to beat Ke Jie, world Go champion in 2017



Advanced Analytics

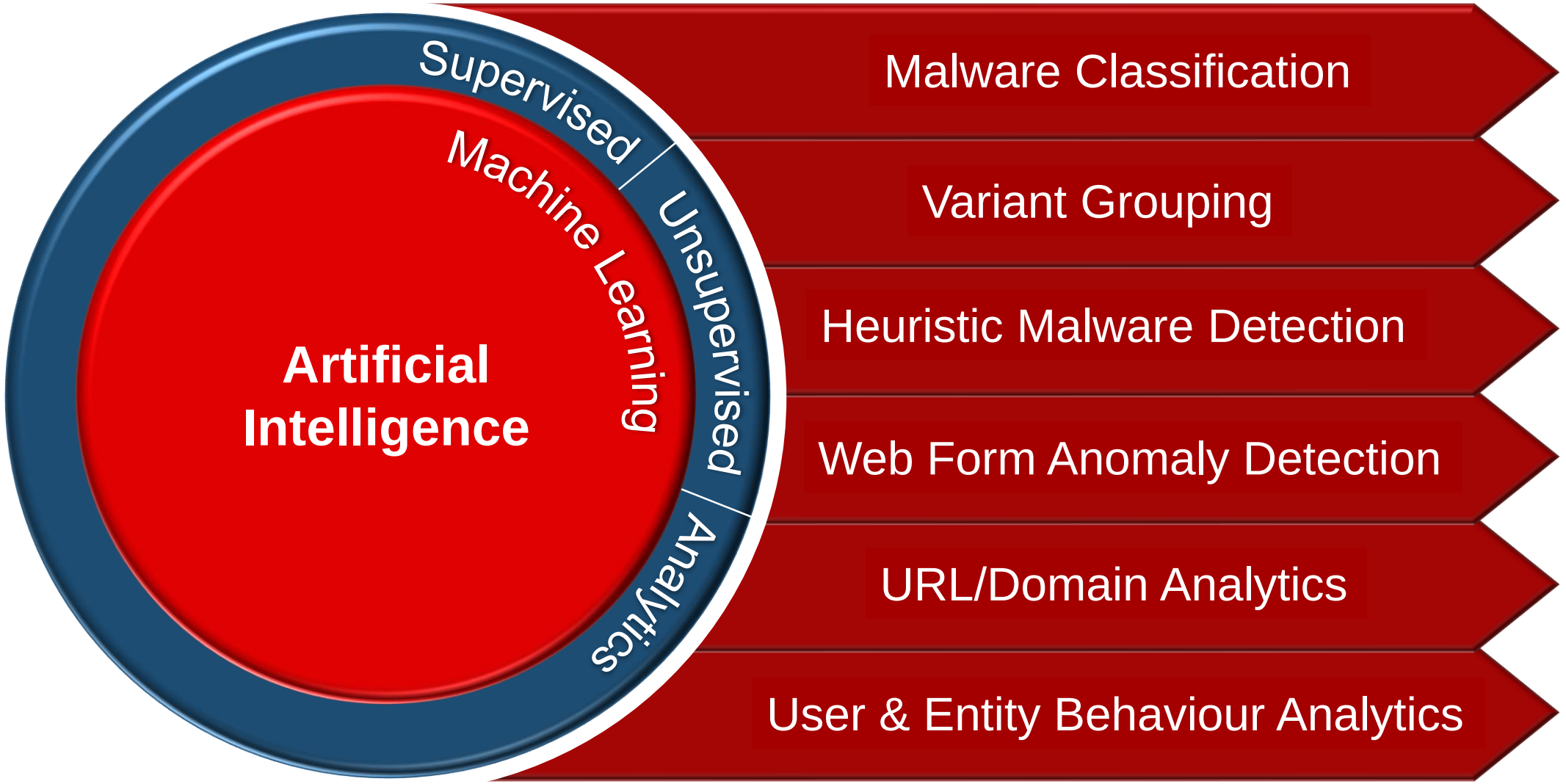
- Analytics is the science of extracting useful information from bulk data
- Advanced analytics is the application of AI to analytics



Artificial Intelligence in FortiGuard

SECURITYDAY

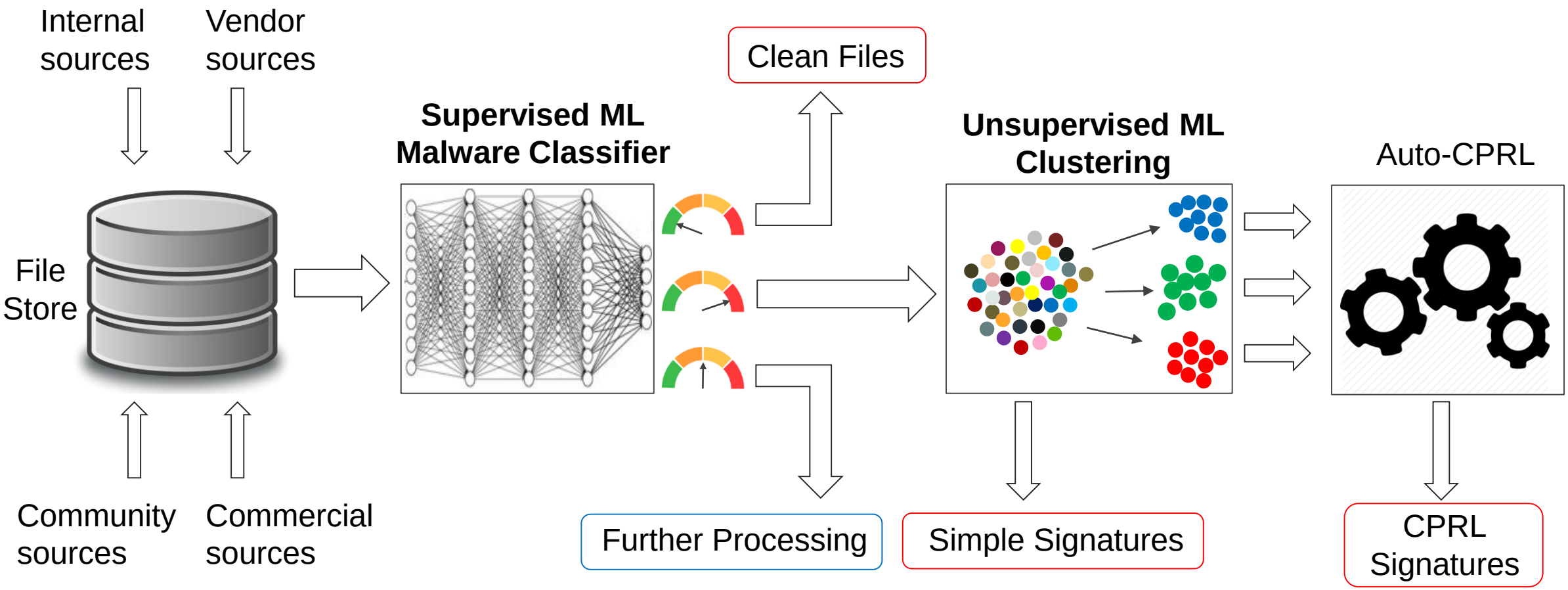
FortiGuard AI



Case Study 1: Malware Processing

- FortiGuard processes around 1.5 million “malicious” files per day
- Around half come from internal sources
- Others are received from third parties
  - » Quality varies, but many received files are **not malicious**
- Checking these files takes a lot of processing

AI-based Malware Processing



Case Study 2: Web Application Security

verizon

#1

Attack pattern leading to a data breach in 2017[1]

EQUIFAX

147.9m

US citizens' personal info stolen in 2017 web application breach

acunetix

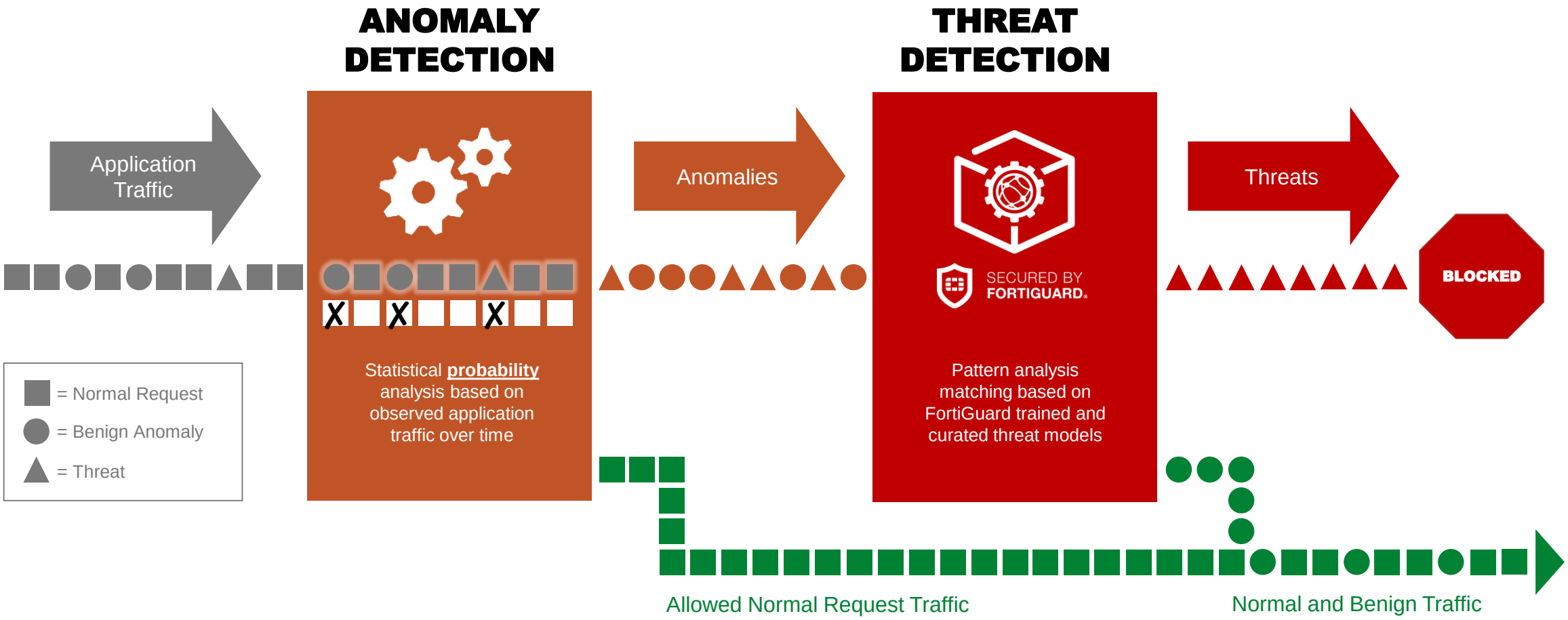
42%

Of all websites have at least one severe vulnerability[2]

Notes/Sources:

1. Verizon 2018 Data Breach Report.
2. Acunetix Web Application Vulnerability Report 2017.

FortiWeb Employs 2 Layers of Machine Learning



v1