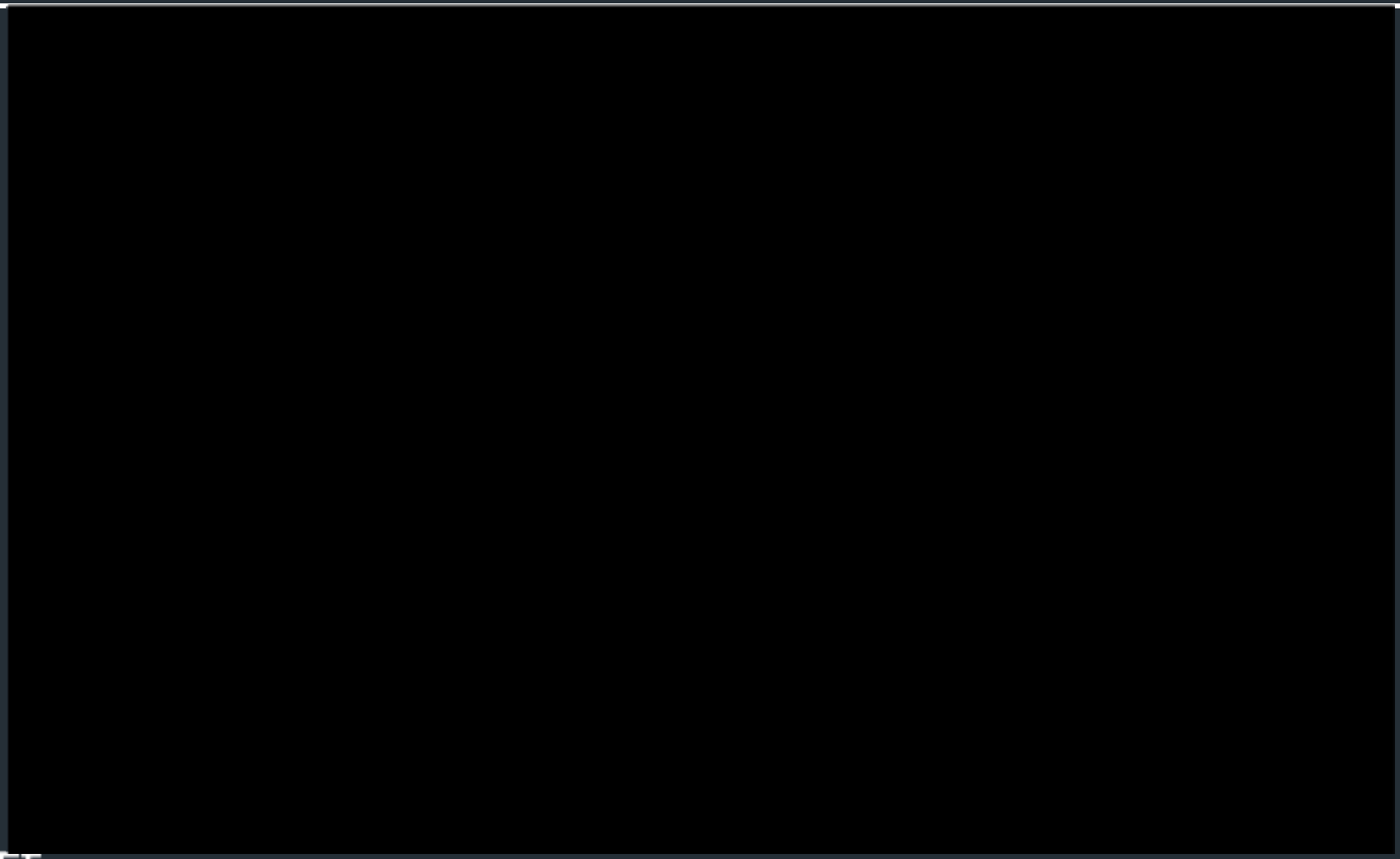
Fighting Cybercrime with AI

Toan Trinh

How Many Passes Does the White Team Make?



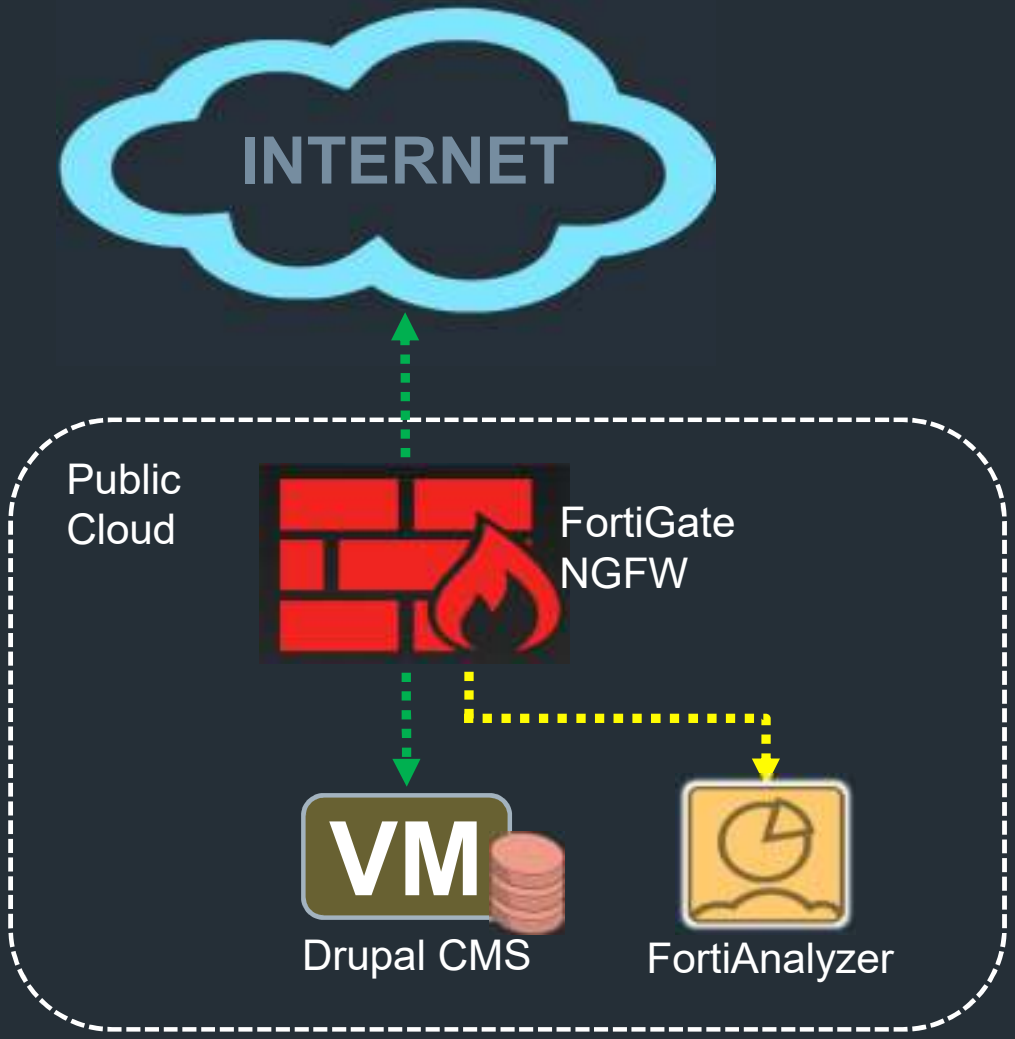

Why Hackers Love The Cloud
CSO
The hackers are coming: 6 cloud computing trends you will see in 2018
Growth is good, and will bring many changes to the cloud industry. But not all changes will be good, especially when it comes to security.
Databases in the cloud - a new target for cyber criminals
exploit vulnerabilities in DBaaS
CLOUDTECH
IoT TECH EXPO GLOBAL 2018
How cloud storage became a target for hackers – and what can be done about it
By David Midgley
Why are hackers increasingly targeting cloud?
Danny Palmer investigates why cyber criminals see cloud as an increasingly lucrative target
QUARTZ
Why the cloud is an attractive target for sophisticated hackers
$5.85 MM

Live Test

Drupal CMS deployed on a Linux Instance

FortiGate NGFW in **Monitoring Mode**

FortiAnalyzer for Centralized Reporting



Day 1

Add Filter | All Devices | Custom... | May 02 To May 03

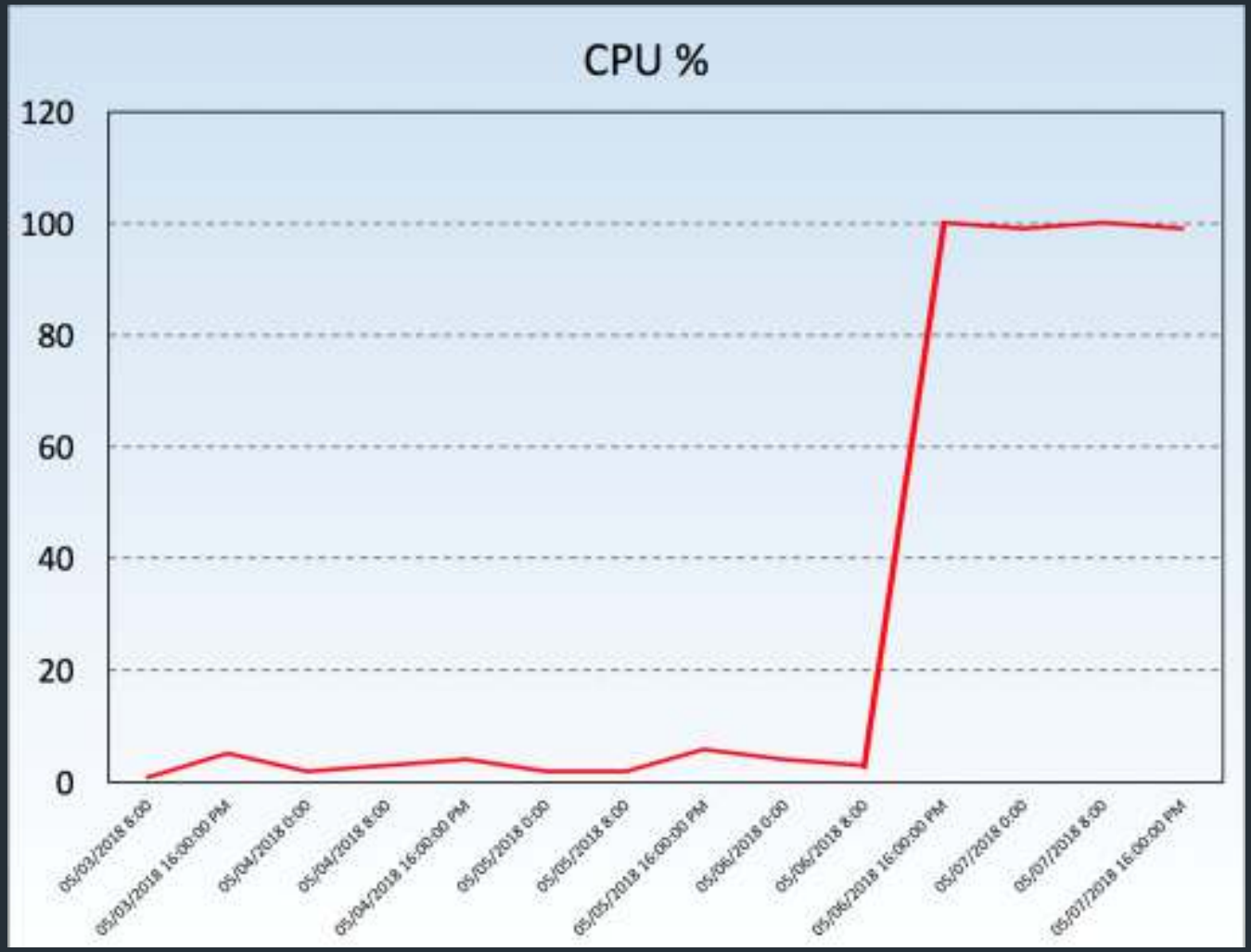
#	Threat	Category	Threat Level
1	MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow	IPS: CVE-2017-7269	Critical
2	Oracle.WebLogic.Server.wls-wsat.Component.Code.Injection	IPS	Critical
3	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	IPS	Critical
4	Failed Connection Attempts	Failed Connection Attempts	Low

Day 5

Add Filter | All Devices | Custom... | May 02 To May 07

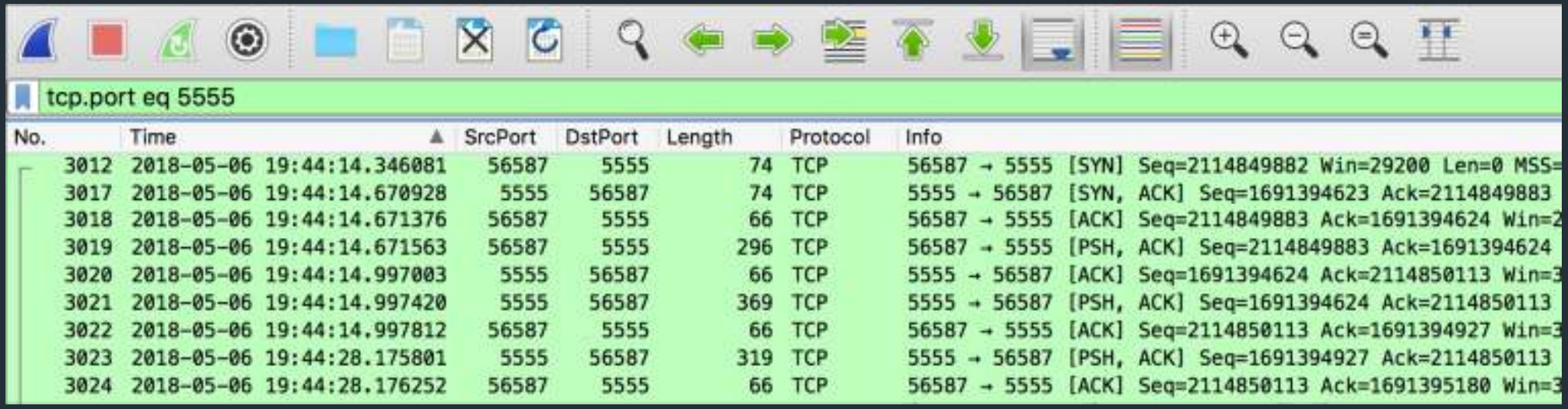
#	Threat	Category	Threat Level
1	Drupal.Core.Form.Rendering.Component.Remote.Code.Execution	IPS	Critical
2	Oracle.WebLogic.Server.wls-wsat.Component.Code.Injection	IPS	Critical
3	MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow	IPS: CVE-2017-7269	Critical
4	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	IPS	Critical
5	Linksys.Routers.Administrative.Console.Authentication.Bypass	IPS	High
6	Proxy.HTTP	Proxy	Medium
7	D-Link.DIR.800.Series.getcfg.php.Information.Disclosure	IPS	Medium
8	Failed Connection Attempts	Failed Connection Attempts	Low
9	ZmEu.Vulnerability.Scanner	IPS	Low
10	Masscan.Scanner	IPS	Low

Drupal Instance CPU Utilization

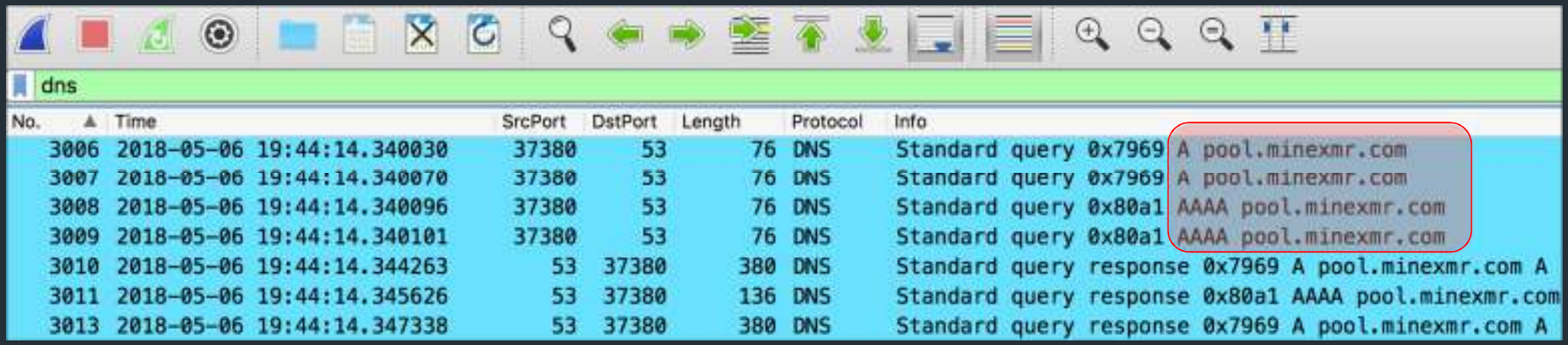


Suspicious Process

```
@drupalserver:/var/log/apache2# netstat -ntap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1013/sshd
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      3736/mysqld
tcp        0      0                 :56587                  :5555       ESTABLISHED 9387/
tcp        0    296                 :22                     :54787      ESTABLISHED 13686/sshd: ubuntu
tcp6       0      0 :::22                   :::*                    LISTEN      1013/sshd
tcp6       0      0 :::80                   :::*                    LISTEN      8009/apache2
```



Crypto-Jacking



dns

No.	Time	SrcPort	DstPort	Length	Protocol	Info
3006	2018-05-06 19:44:14.340030	37380	53	76	DNS	Standard query 0x7969 A pool.minexmr.com
3007	2018-05-06 19:44:14.340070	37380	53	76	DNS	Standard query 0x7969 A pool.minexmr.com
3008	2018-05-06 19:44:14.340096	37380	53	76	DNS	Standard query 0x80a1 AAAA pool.minexmr.com
3009	2018-05-06 19:44:14.340101	37380	53	76	DNS	Standard query 0x80a1 AAAA pool.minexmr.com
3010	2018-05-06 19:44:14.344263	53	37380	380	DNS	Standard query response 0x7969 A pool.minexmr.com A
3011	2018-05-06 19:44:14.345626	53	37380	136	DNS	Standard query response 0x80a1 AAAA pool.minexmr.com
3013	2018-05-06 19:44:14.347338	53	37380	380	DNS	Standard query response 0x7969 A pool.minexmr.com A

What do you think happened?

Vulnerability Targeting

94% Published Vulnerabilities Are Never Exploited

Q2 – 122 new CVE's published – 4 Targeted

Cryptojacking – Region Distribution

FortiGuard AI

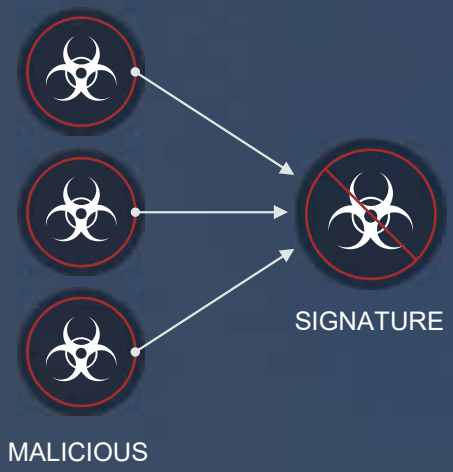
FORTINET SECURITYWORLD2018

Known Protection

Unknown Detection

ONE TO ONE SIGNATURE

ONE TO MANY SIGNATURE

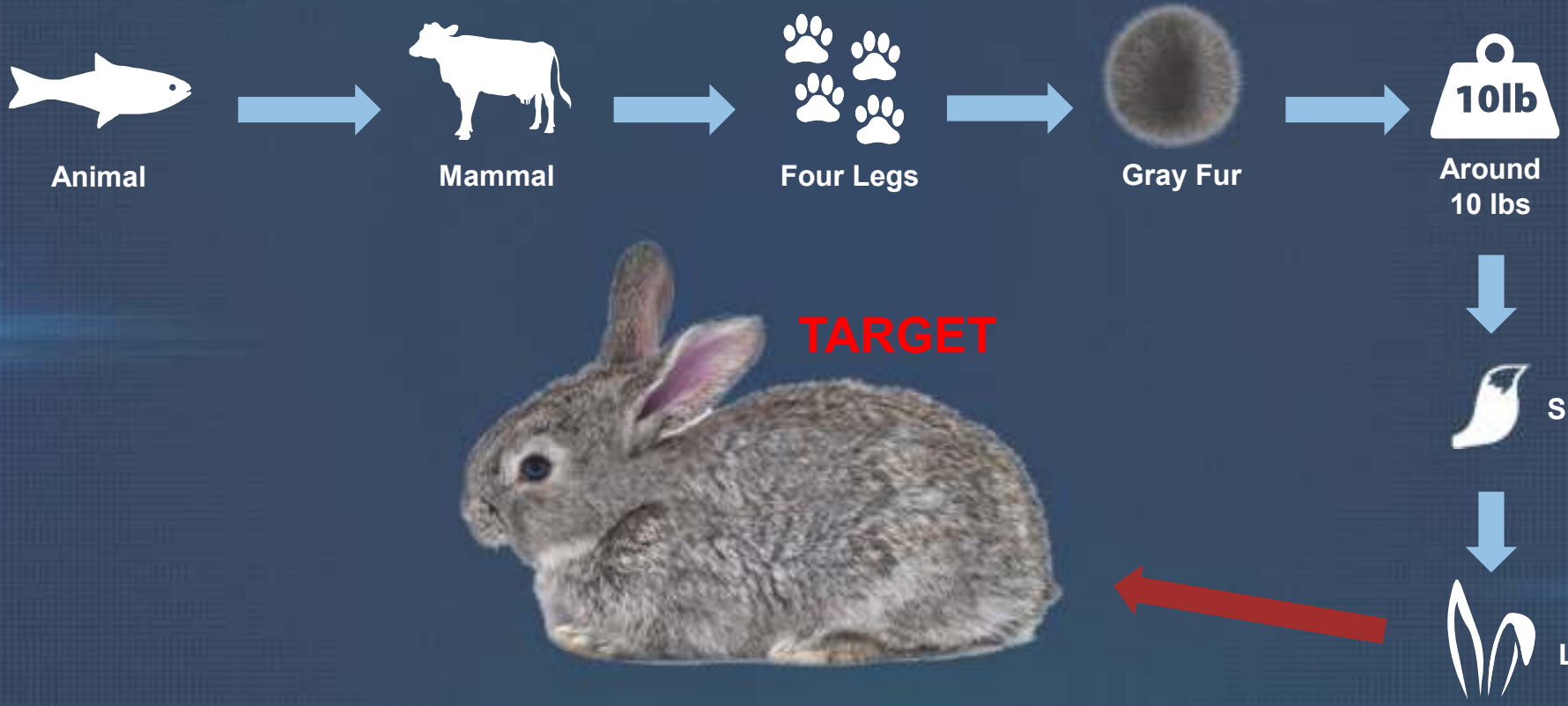


BEHAVIORAL ANALYSIS

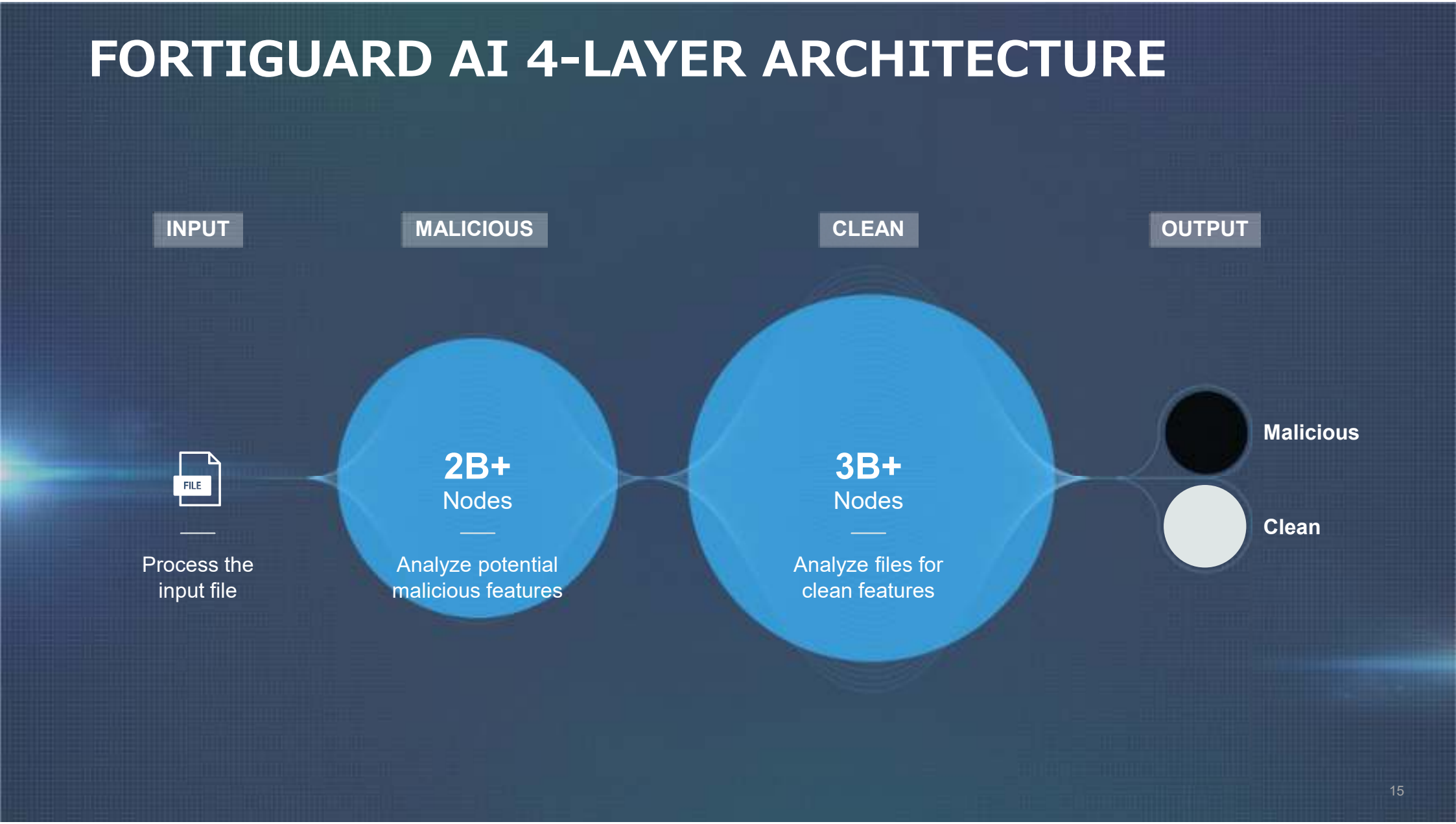
DEEP LEARNING

Machine Learning 101

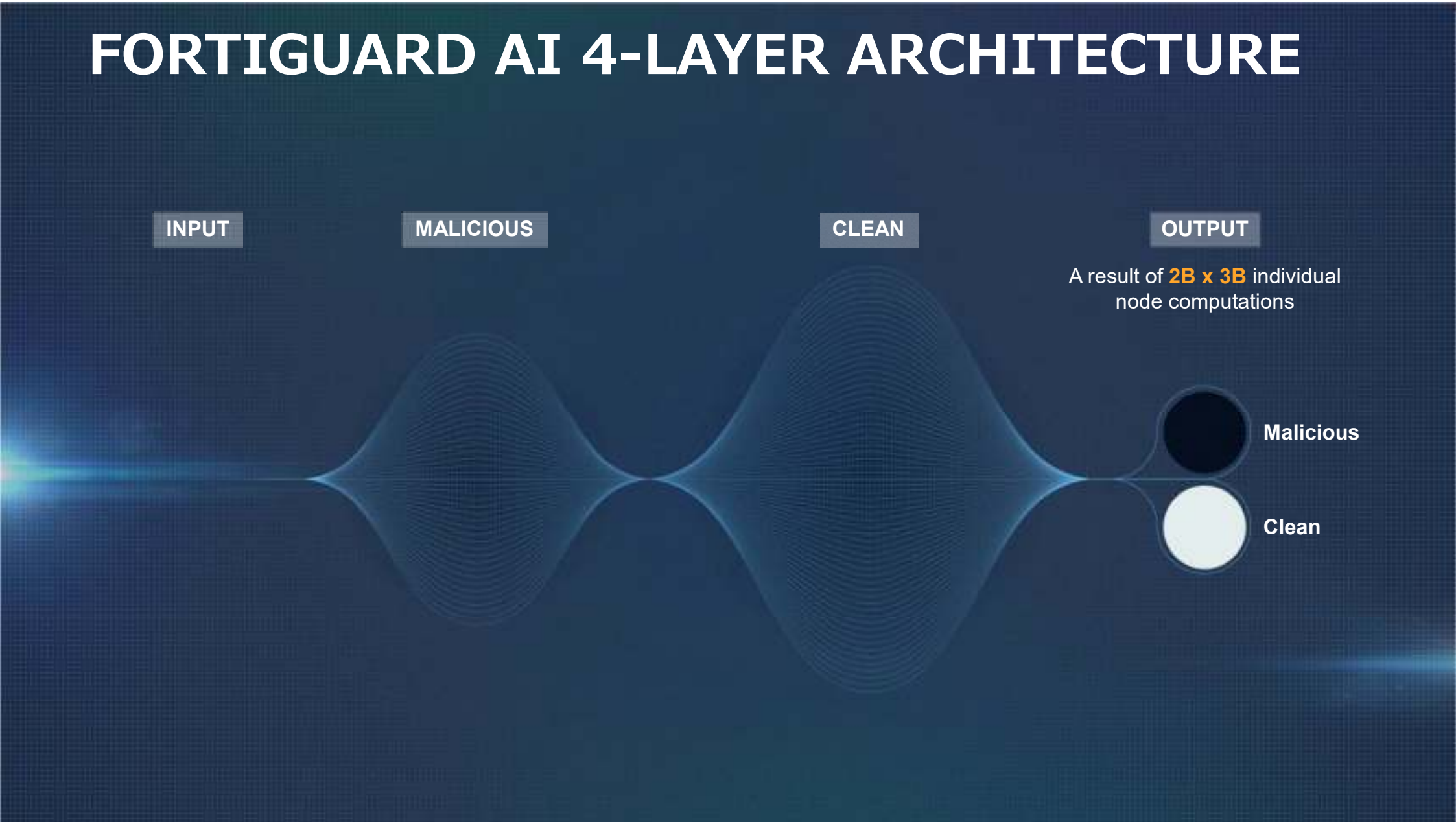
FEATURE EXTRACTION – DETERMINE THE OBJECT



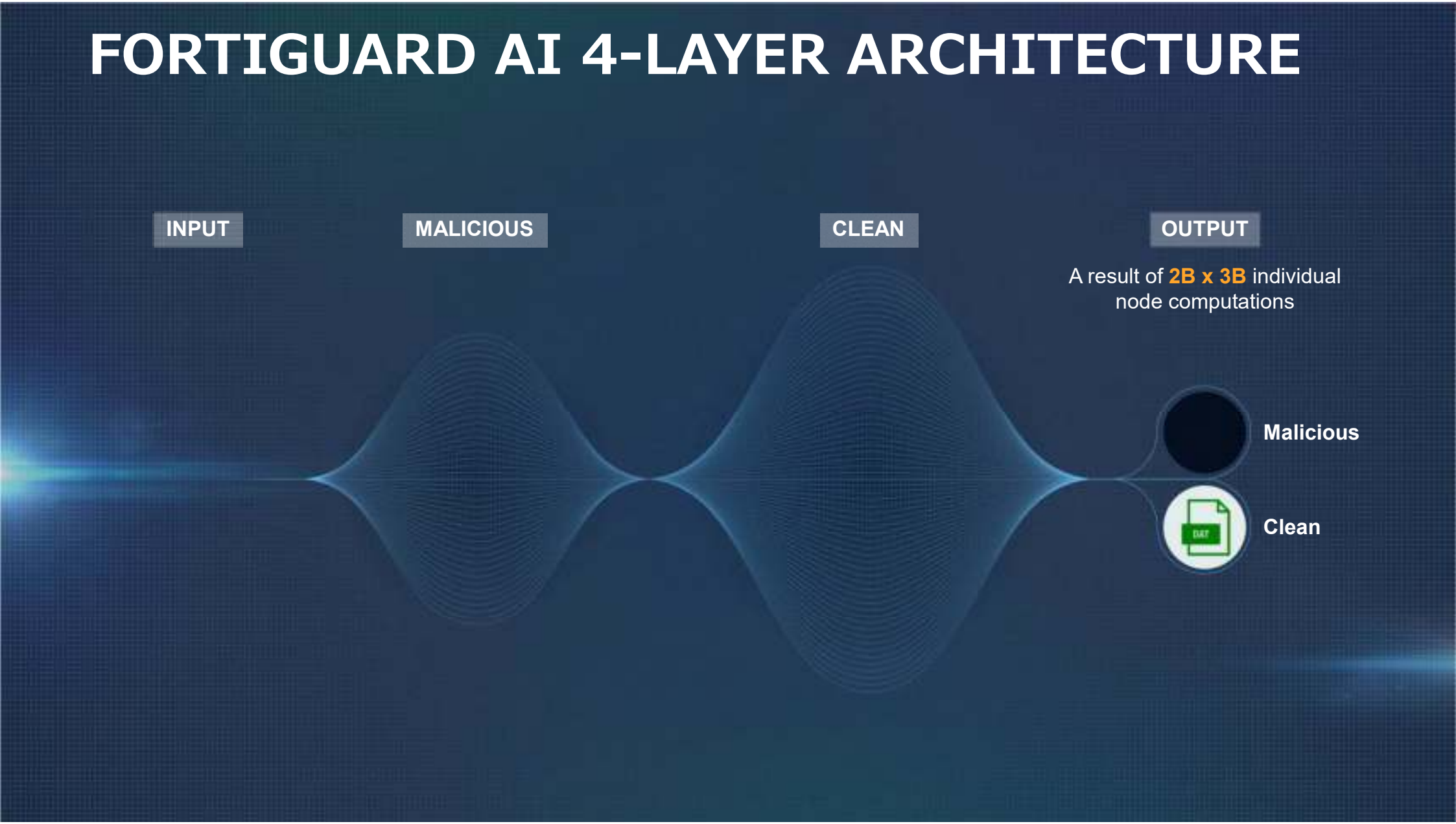
FORTIGUARD AI 4-LAYER ARCHITECTURE



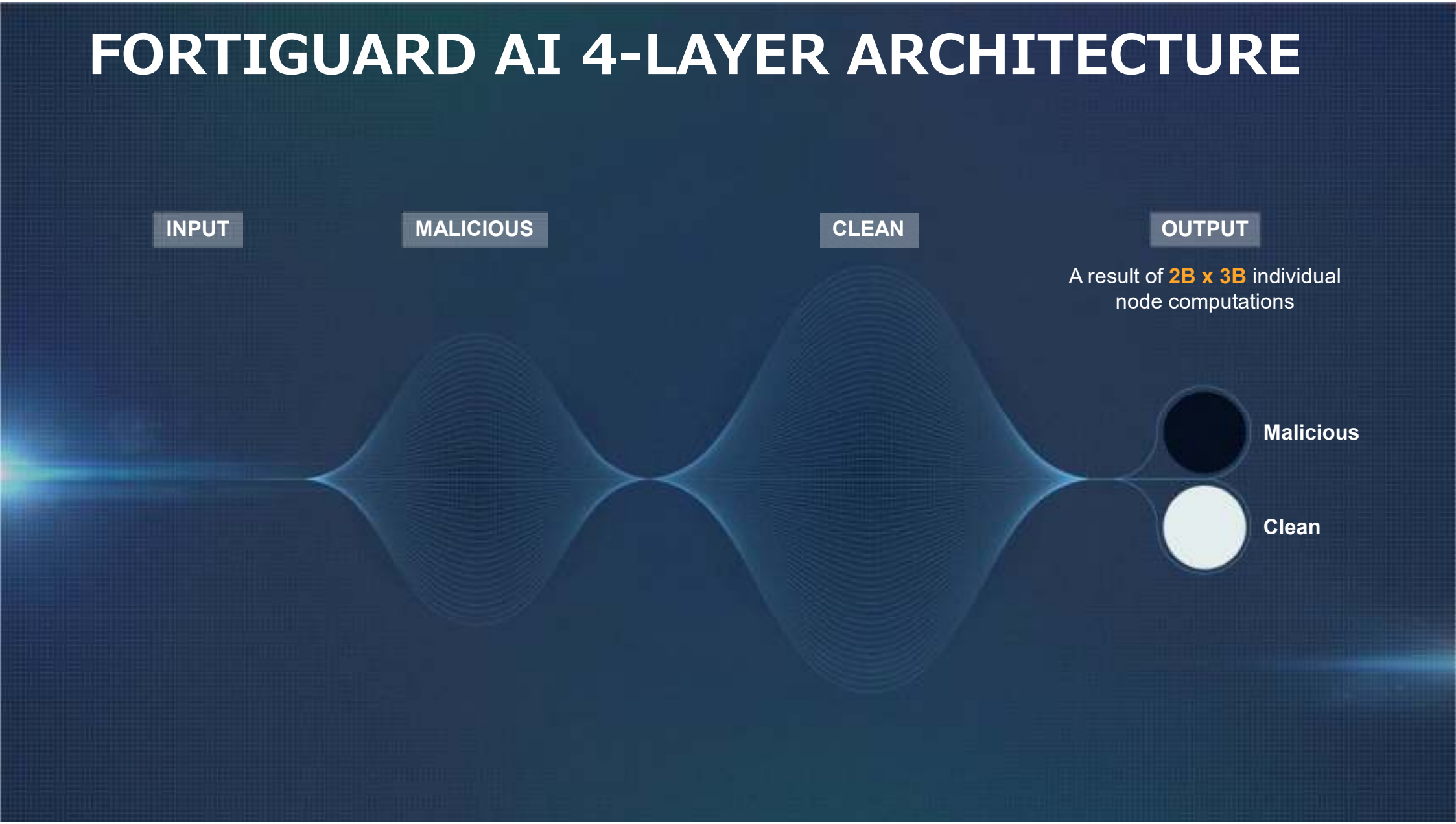
FORTIGUARD AI 4-LAYER ARCHITECTURE



FORTIGUARD AI 4-LAYER ARCHITECTURE

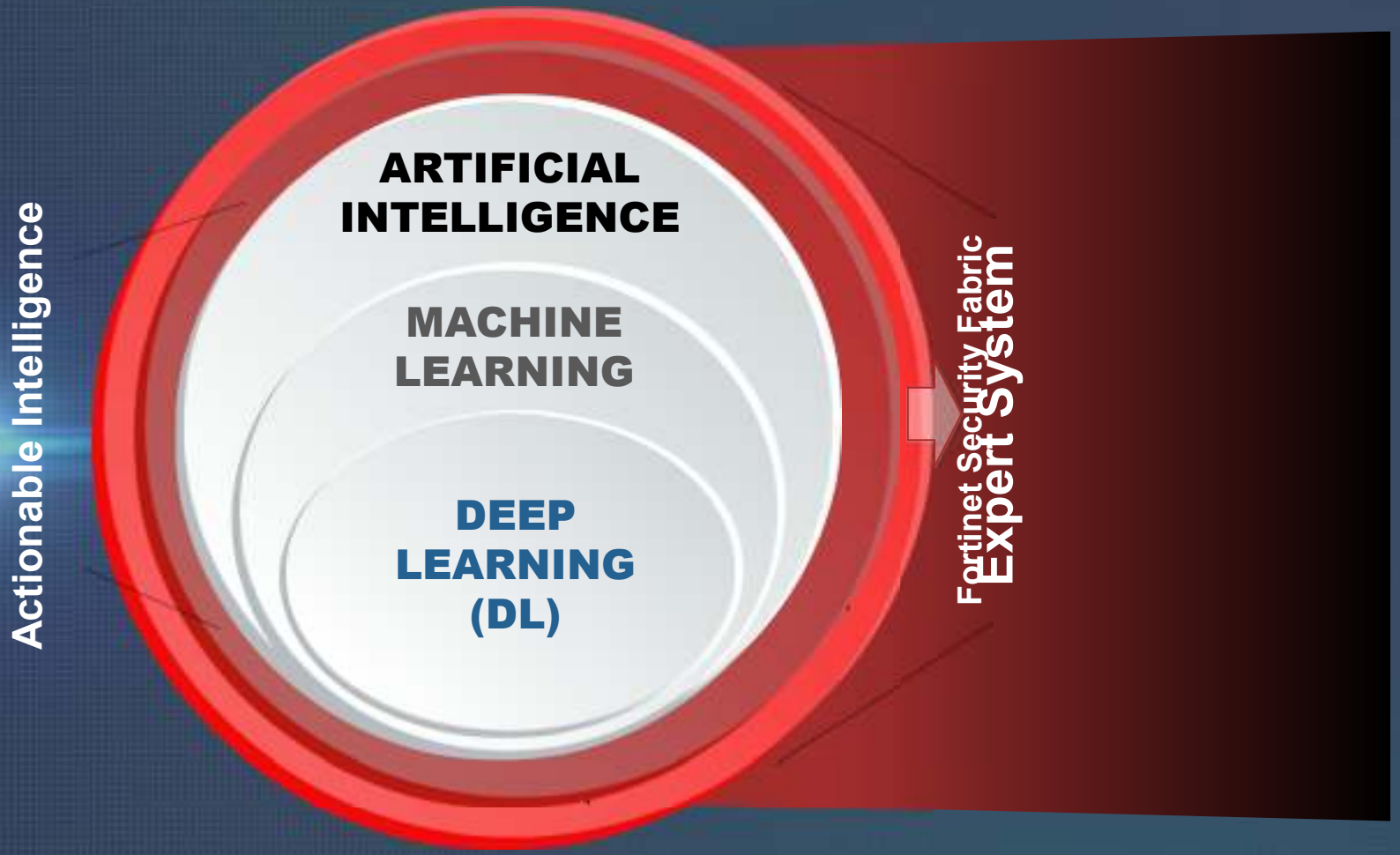


FORTIGUARD AI 4-LAYER ARCHITECTURE

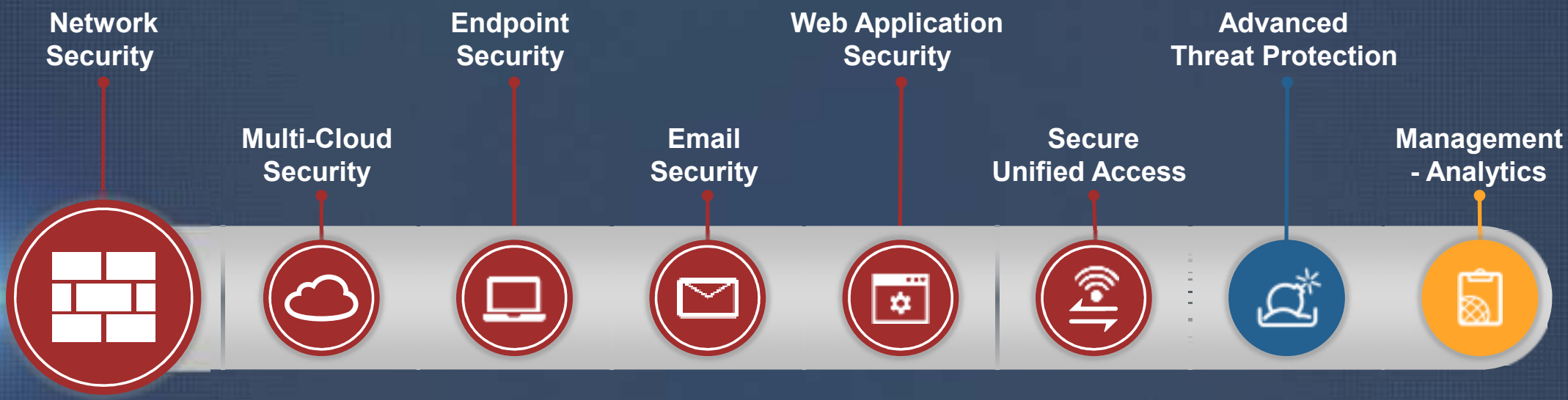


Fortinet & FortiGuard: The Expert System

Crossing the “Last Mile”: Creating Actionable Intelligence

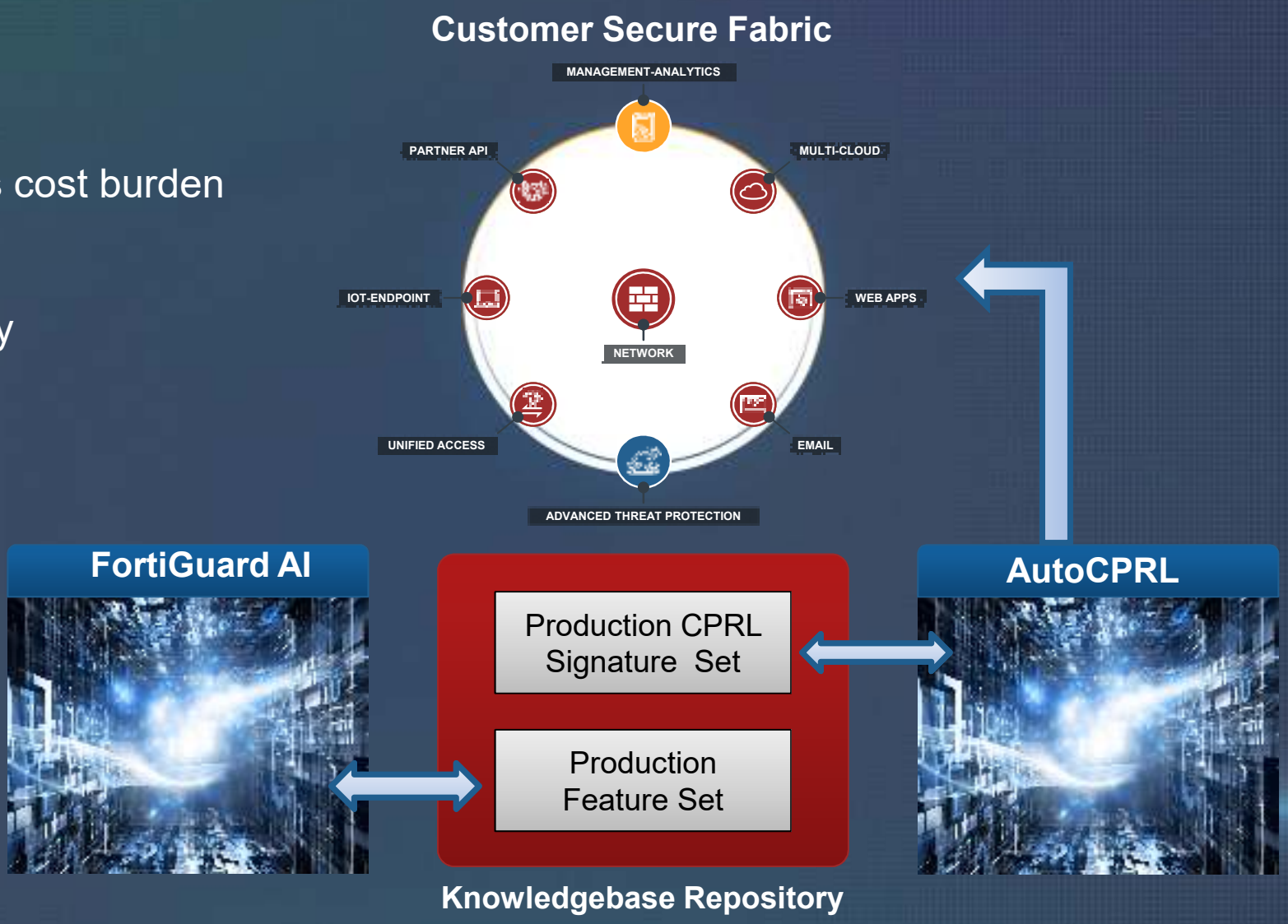


2018 Fortinet Solutions



The Result

- Significantly increases cost burden for cybercriminals
- Unsurpassed accuracy
- Proven and validated
- Extremely adaptive



FortiGuard Threat Intelligence Projects

CISCP
& NCCIC

How can I start using FortiGuard AI?

Cyber Threat Assessment Program

- Augments existing solutions
- Each assessment highlights

- » Application vulnerabilities
- » Malware/botnet detection
- » At risk devices within the network

- » Application categories and cloud usage
- » Peer to peer, proxy app and remote access
- » Web-based applications and browsing habits

- » Bandwidth analysis and top consumers
- » Sizing information – average log rates/sessions
- » FortiGate CPU and memory utilization


FORTINET