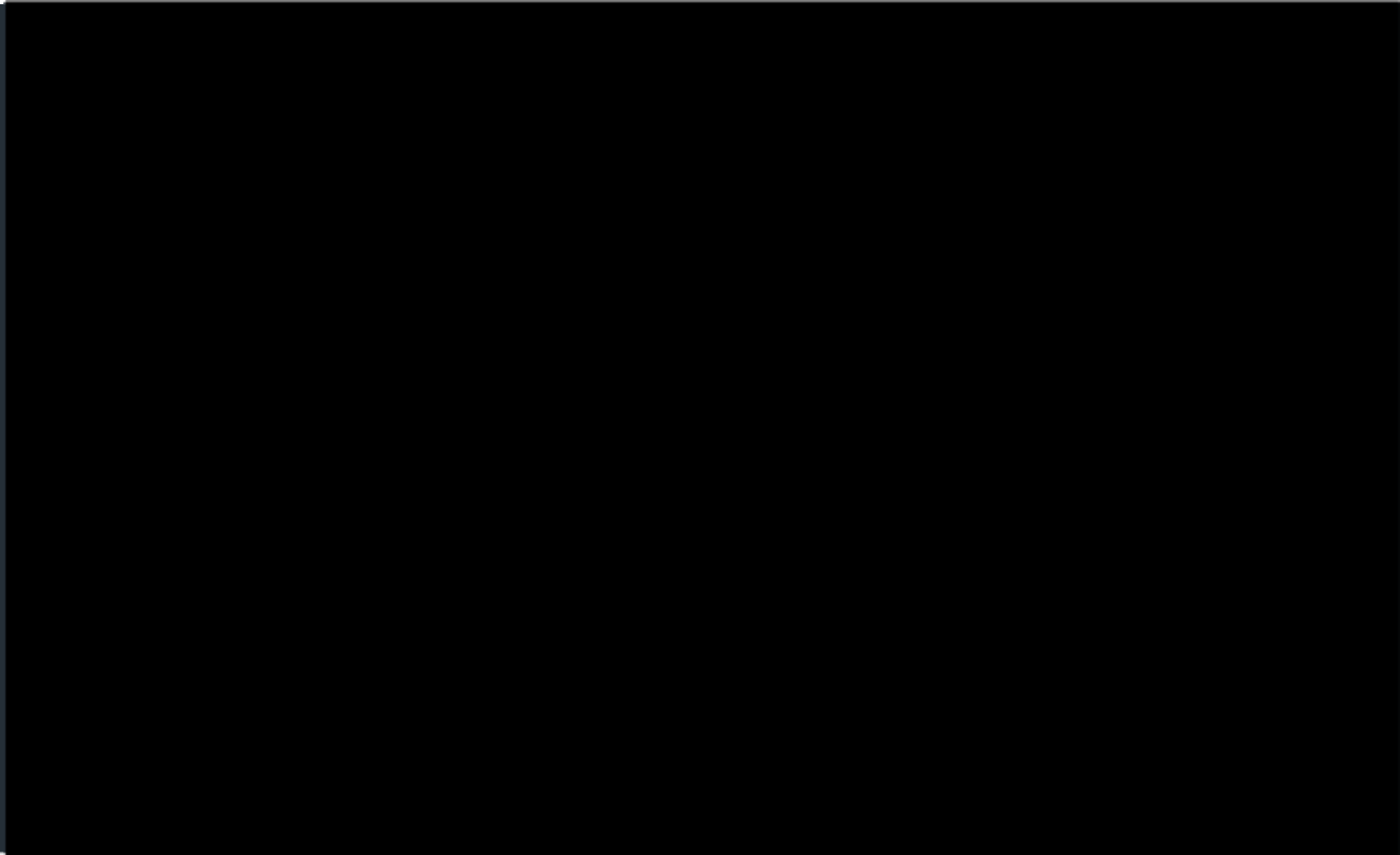


Fighting Cybercrime with AI

Toan Trinh

How Many Passes Does the White Team Make?



FOX

Why Hackers Love The Cloud



For a skilled hacker, a major company's cloud system is a treasure trove — sensitive data, including millions of bank account logs, email addresses and social security numbers can be just a few clicks away.

CSO Sign In | Register

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.

[f](#) [in](#) [G+](#) [v](#) [e](#) [m](#) [t](#)

Databases in the cloud - a new target for cyber criminals



exploit vulnerabilities in DBaaS

Why are hackers increasingly targeting cloud?

Danny Palmer investigates why cyber criminals see cloud as an increasingly lucrative target



CLOUDTECH **IoT TECH EXPO GLOBAL 2018**

How cloud storage became a target for hackers – and what can be done about it

By David Midgley
20 October 2016, 11:01 p.m.



With the recent revelations that Yahoo! experienced a hack in 2014 where the accounts of around 500 million users were compromised, it brings back into focus the importance of businesses ensuring their customers' data is always protected.

QUARTZ

Why the cloud is an attractive target for sophisticated hackers

\$5.85 MM

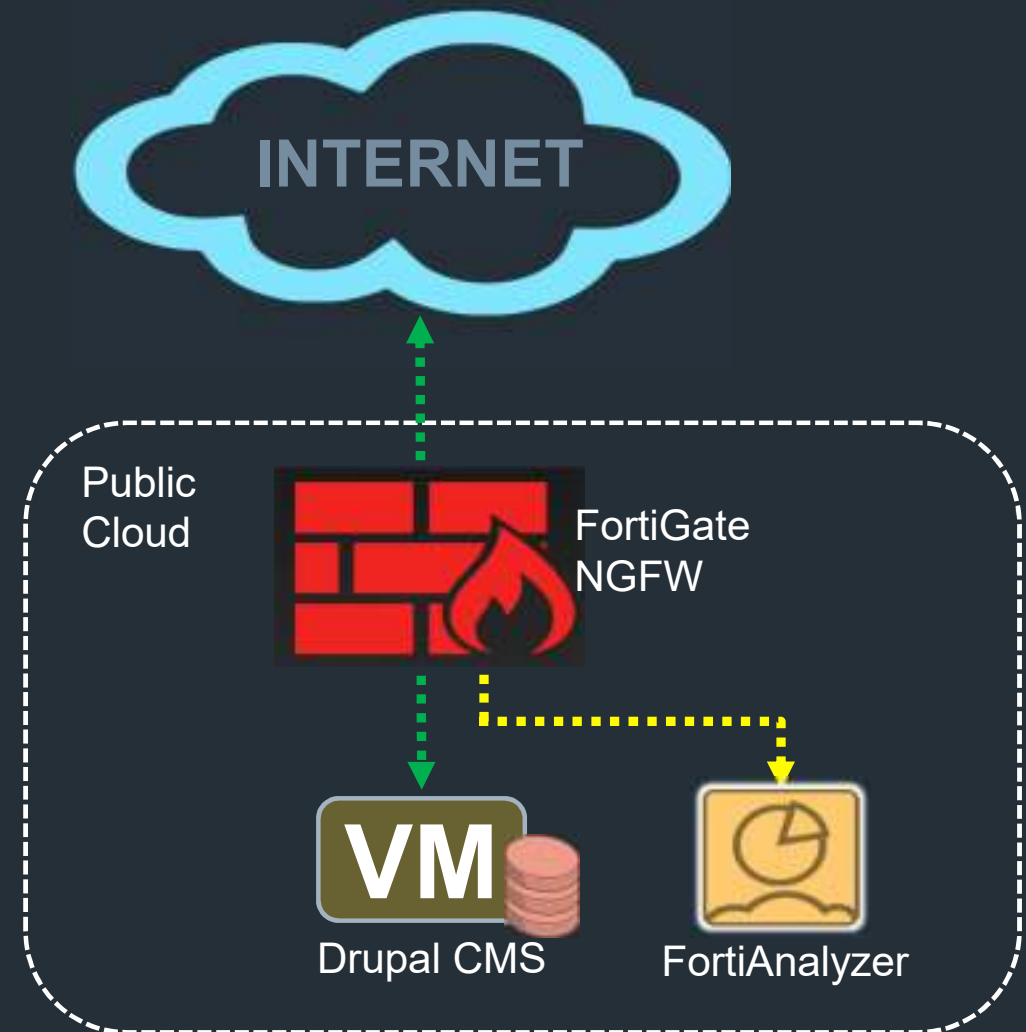
AVERAGE TOTAL ORGANIZATIONAL COST OF A DATA BREACH IN THE U.S. Q3/16*

Live Test

Drupal CMS deployed on a Linux Instance

FortiGate NGFW in **Monitoring Mode**

FortiAnalyzer for Centralized Reporting



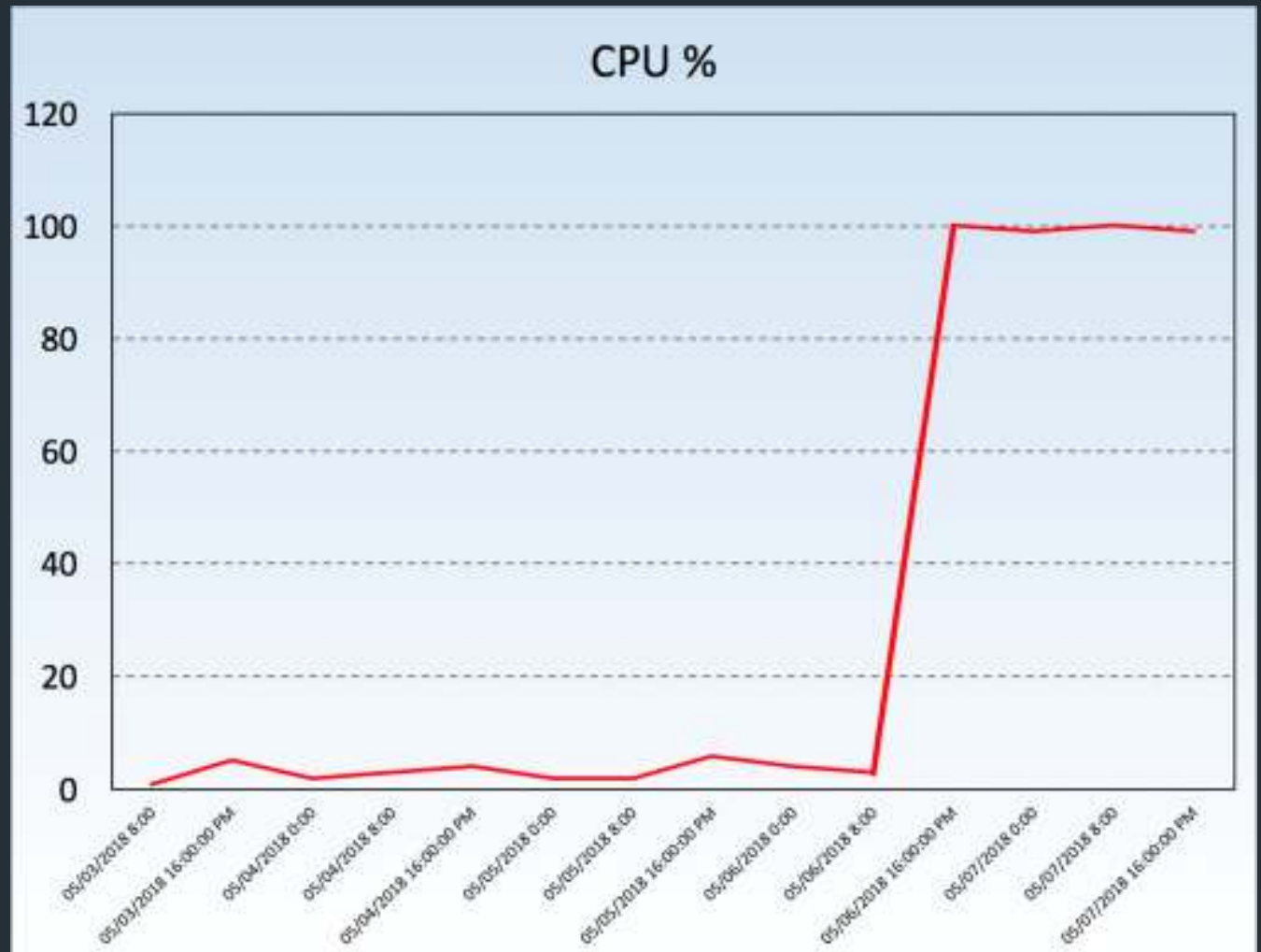
Day 1

#	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

#	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

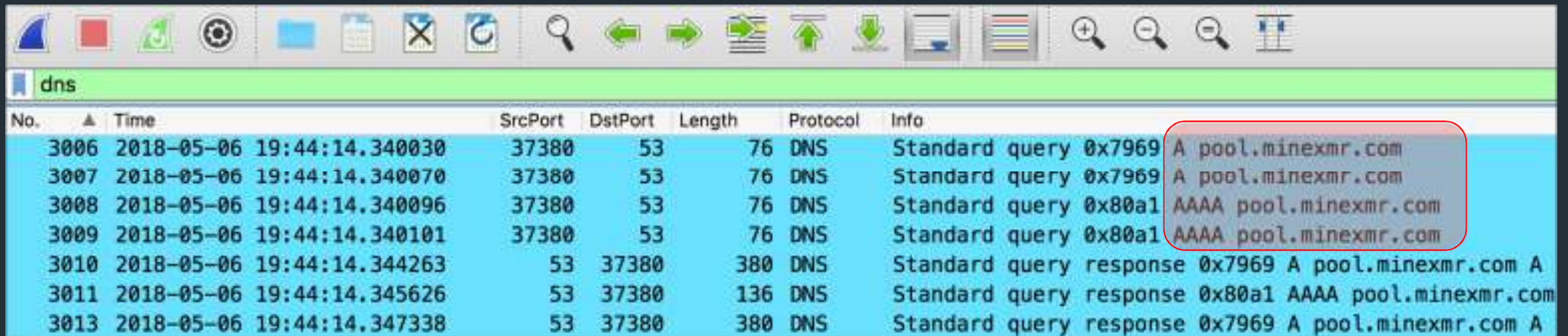
```
@drupalserver:/var/log/apache2# netstat -ntap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1013/sshd
tcp      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



tcp.port eq 5555

No.	Time	SrcPort	DstPort	Length	Protocol	Info
3012	2018-05-06 19:44:14.346081	56587	5555	74	TCP	56587 → 5555 [SYN] Seq=2114849882 Win=29200 Len=0 MSS=
3017	2018-05-06 19:44:14.670928	5555	56587	74	TCP	5555 → 56587 [SYN, ACK] Seq=1691394623 Ack=2114849883
3018	2018-05-06 19:44:14.671376	56587	5555	66	TCP	56587 → 5555 [ACK] Seq=2114849883 Ack=1691394624 Win=2
3019	2018-05-06 19:44:14.671563	56587	5555	296	TCP	56587 → 5555 [PSH, ACK] Seq=2114849883 Ack=1691394624
3020	2018-05-06 19:44:14.997003	5555	56587	66	TCP	5555 → 56587 [ACK] Seq=1691394624 Ack=2114850113 Win=3
3021	2018-05-06 19:44:14.997420	5555	56587	369	TCP	5555 → 56587 [PSH, ACK] Seq=1691394624 Ack=2114850113
3022	2018-05-06 19:44:14.997812	56587	5555	66	TCP	56587 → 5555 [ACK] Seq=2114850113 Ack=1691394927 Win=3
3023	2018-05-06 19:44:28.175801	5555	56587	319	TCP	5555 → 56587 [PSH, ACK] Seq=1691394927 Ack=2114850113
3024	2018-05-06 19:44:28.176252	56587	5555	66	TCP	56587 → 5555 [ACK] Seq=2114850113 Ack=1691395180 Win=3

Crypto-Jacking



The image shows a Wireshark network traffic capture window titled 'dns'. The table below displays the captured packets, highlighting a sequence of DNS queries and responses for the domain 'pool.minexmr.com'. A red box highlights the first three rows, which are standard queries for A and AAAA records.

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?



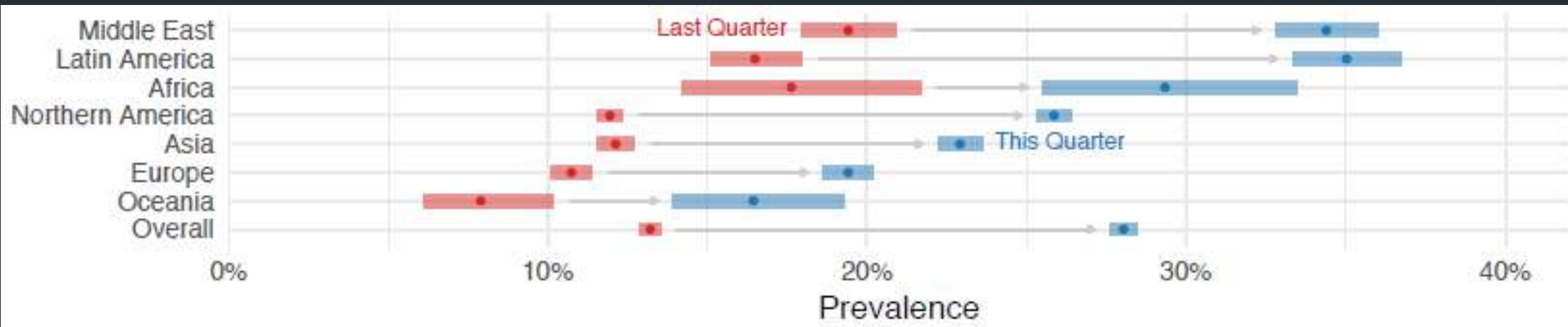
Vulnerability Targeting

94% Published Vulnerabilities Are **Never Exploited**

Q2 – 122 new CVE's published – 4 Targeted



Cryptojacking – Region Distribution



+++
++
+ + +
FortiGuard
AI



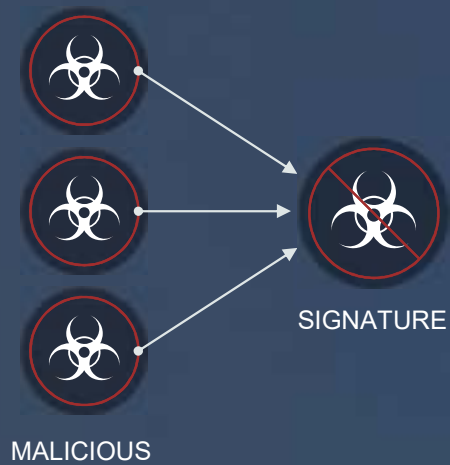
Known Protection

Unknown Detection

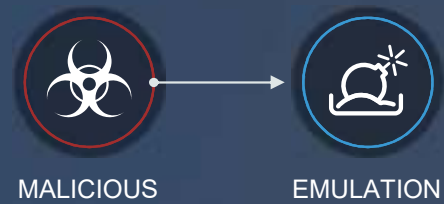
ONE TO ONE SIGNATURE



ONE TO MANY SIGNATURE



BEHAVIORAL ANALYSIS

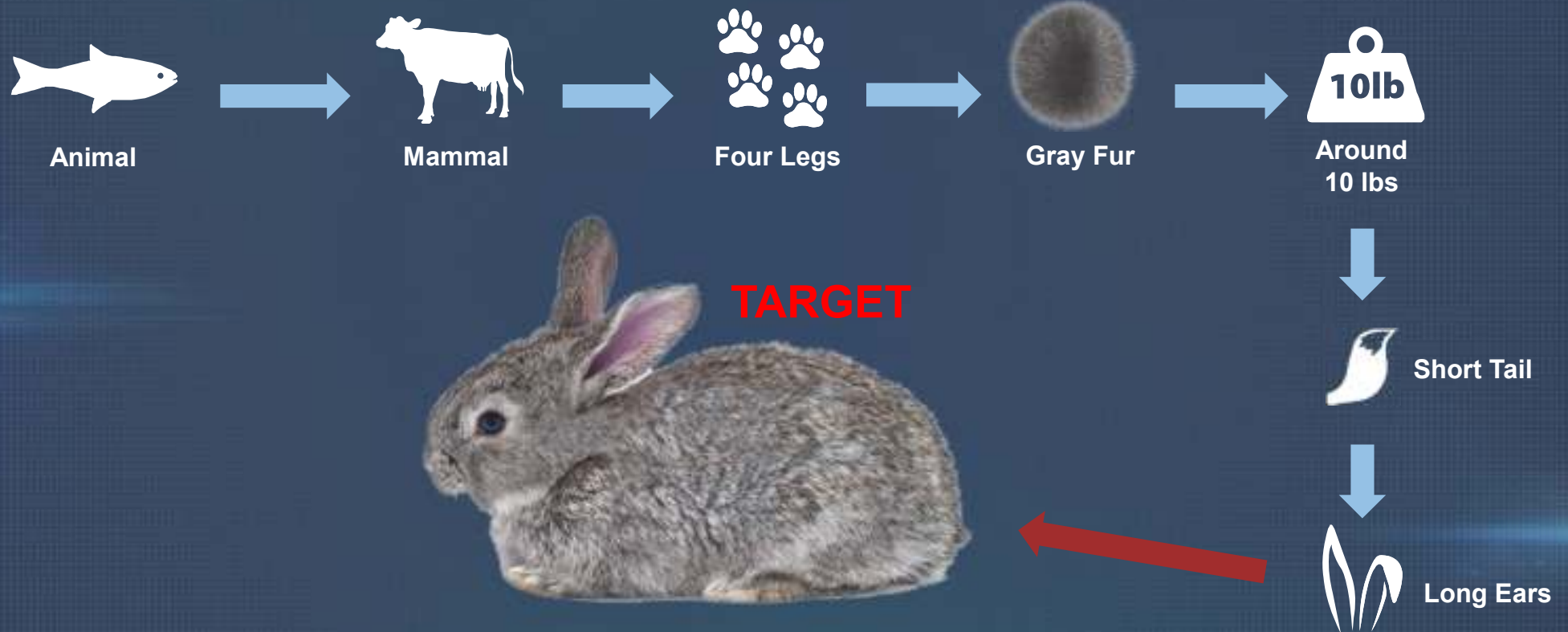


DEEP LEARNING

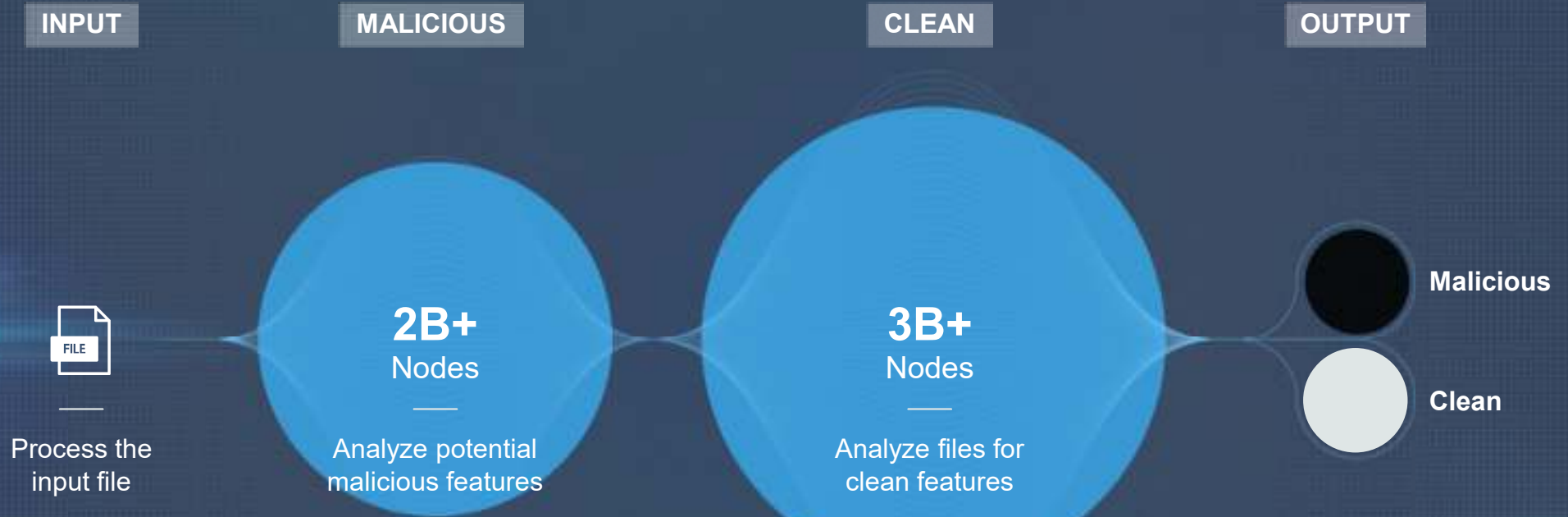


Machine Learning 101

FEATURE EXTRACTION – DETERMINE THE OBJECT



FORTIGUARD AI 4-LAYER ARCHITECTURE



FORTIGUARD AI 4-LAYER ARCHITECTURE

INPUT

MALICIOUS

CLEAN

OUTPUT

A result of **2B x 3B** individual
node computations

Malicious

Clean



FORTIGUARD AI 4-LAYER ARCHITECTURE

INPUT

MALICIOUS

CLEAN

OUTPUT

A result of **2B x 3B** individual node computations



Malicious

Clean

FORTIGUARD AI 4-LAYER ARCHITECTURE

INPUT

MALICIOUS

CLEAN

OUTPUT

A result of **2B x 3B** individual
node computations

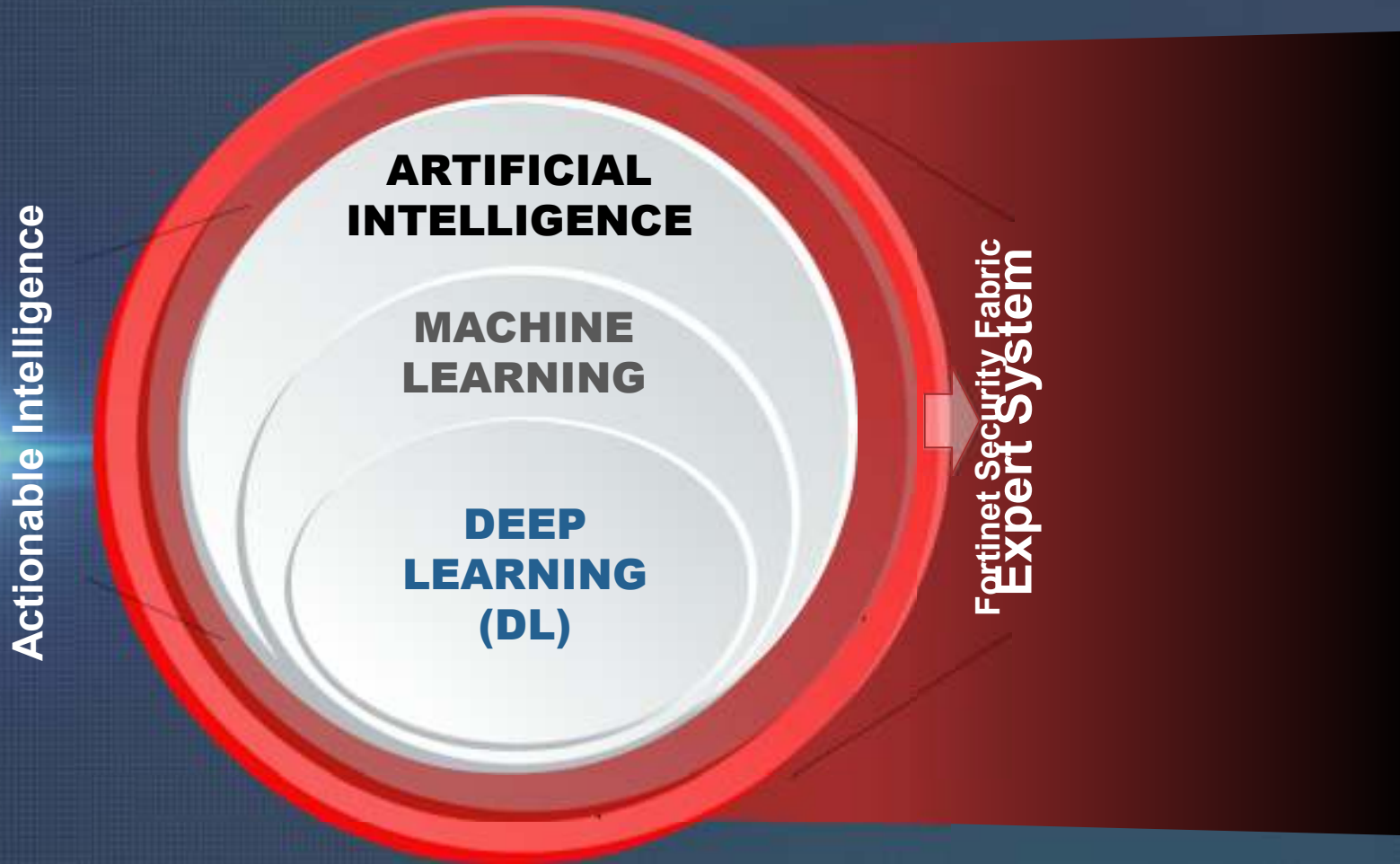
Malicious

Clean



Fortinet & FortiGuard: The Expert System

Crossing the “Last Mile”: Creating Actionable Intelligence

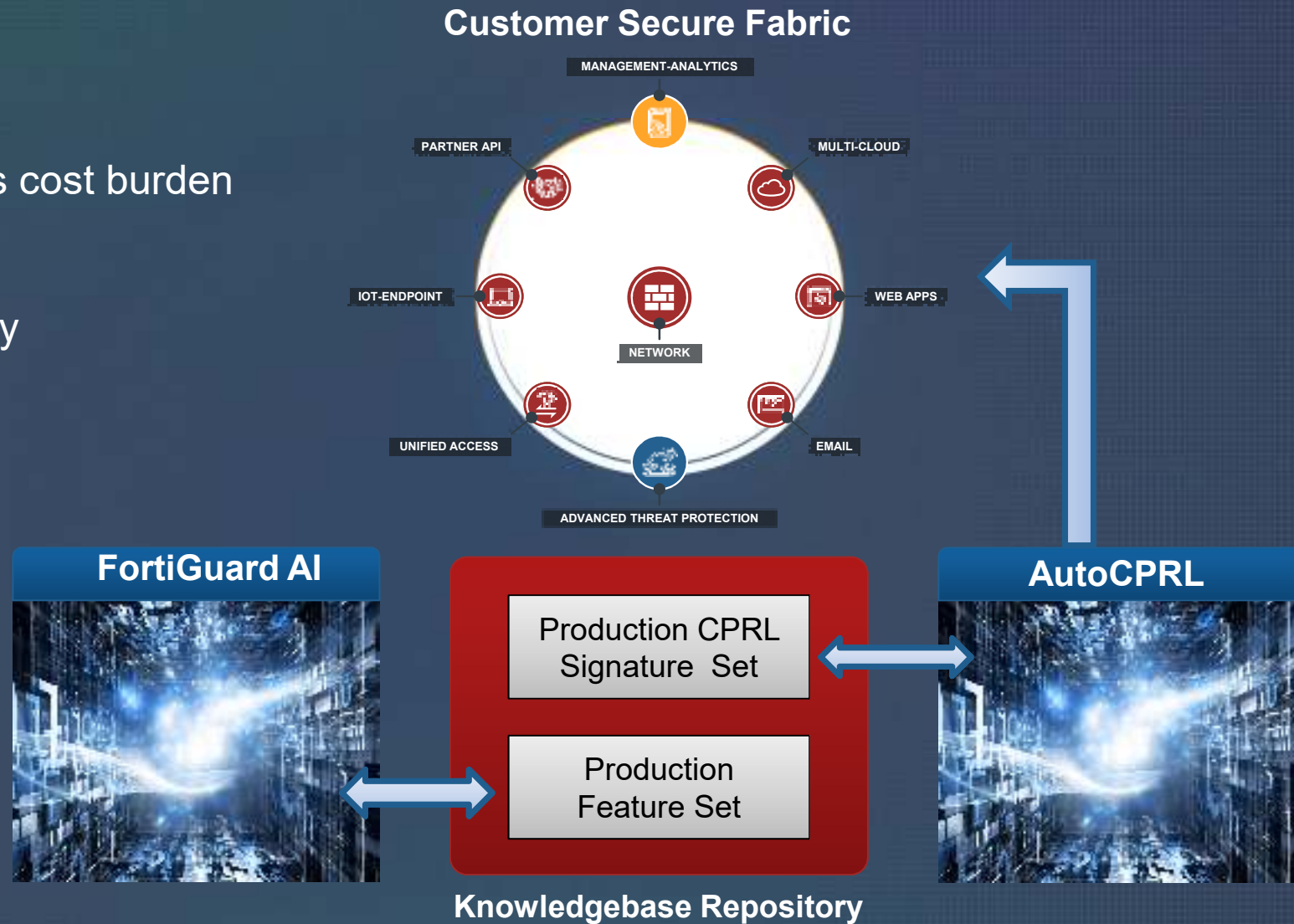


2018 Fortinet Solutions



The Result

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



FortiGuard Threat Intelligence Projects



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



The image features a dark blue background with faint, light-colored molecular structures and network diagrams. The central focus is the word "FERTINET" in a bold, white, sans-serif font. The letter "E" is stylized with three vertical bars. A registered trademark symbol (®) is located at the end of the word. The background graphics include a complex network of nodes and lines on the right side, and a circular molecular structure on the left side.

FERTINET®