الهيئة الوطنية للإتصالات
Instance Nationale des Telecommunications

Security for the Networks of the Future

SECURE64™

GET Wireless

Issues and challenges of a successful deployment of future networks

14th March - 2018

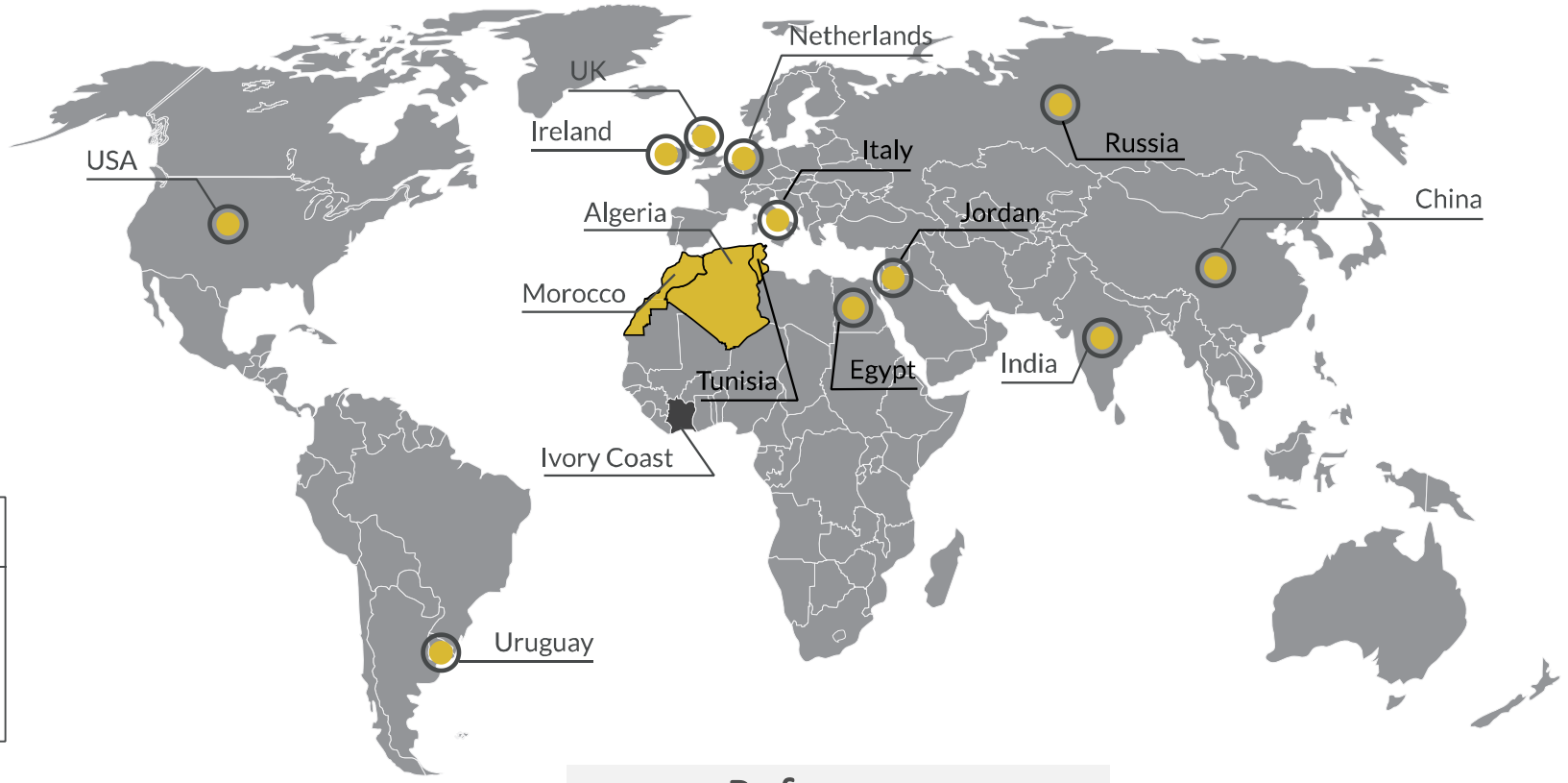
GET Wireless - **At a Glance**

- Founded in 2001
- Head Office in Tunis, Tunisia
- Over 100 employees

- Office in Algiers, Algeria - 2012
- Office in Casa, Morroco - 2015
- Sales Presence in Ivory Coast
- 40 Partners worldwide

GET Wireless – **Partners' Locations & Main References**

الهيئة الوطنية للإتصالات
Instance Nationale des Telecommunications



References

ooredoo · orange · TT اتصالات تونس GROUPE TUNISIE TELECOM · WIS · jordan telecom group · CITIC 1616 · celcom · ERICSSON

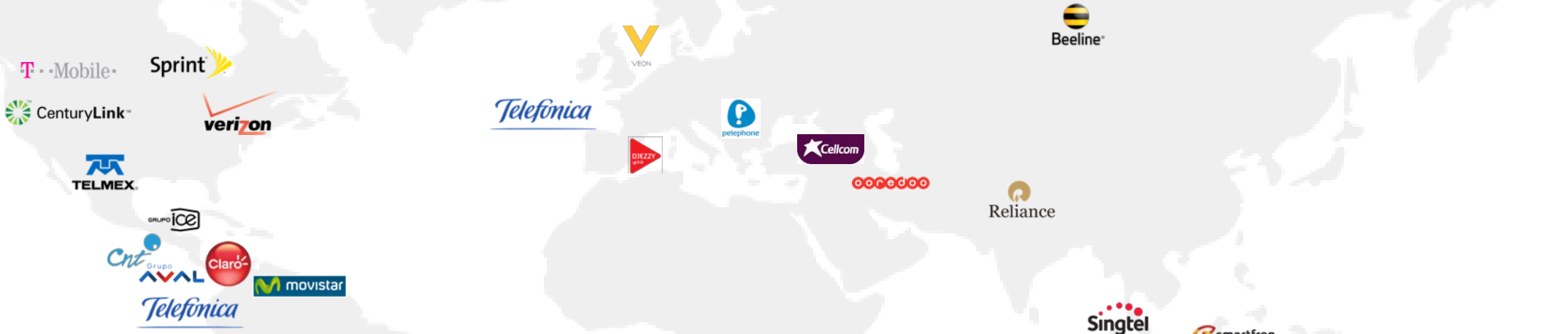
AIRCOM INTERNATIONAL · vodafone · إتصالات الجزائر ALGERIE TELECOM · inwi عبّر كبغيتي · DJEZZY جازي · NOKIA · HUAWEI · Alcatel·Lucent

GET Wireless

SECURE64™

الهيئة الوطنية للإتصالات
Instance Nationale des Telecommunications

Trusted Partner for DNS Security for more than a decade at leading Tier1/2 Operators



+850 Millions End-Users served Worldwide

3 of 5 iana Bodies have already chosen for the Global DNS Internet security

85% of RIR-owned reverse address space signed

Africa Mobilizes

"Mobile technology has transformed African societies"[1]

- **Africa leads the world in money transfers via mobile**[1]

- **Africa grew from 4.5 million internet users in 2000, to approximately 300 million today**[1]

- **Internet use on mobile phones in sub-Saharan Africa is expected to increase 20-fold between the end of 2013 & 2019 – double the rest of the world – to reach 930 million**[2]

1. https://enact-africa.s3.amazonaws.com/site/uploads/2017-09-26-enact-continental-report1.pdf
2. https://www.ericsson.com/res/docs/2014/emr-june2014-regional-appendices-ssa.pdf.

Africa & Cyber crime

"The combination of a growing number of people online combined with weak networks & information security has made Africa particularly vulnerable to attack." [1]

- **49 million cyber attacks took place in Africa in the first quarter of 2014** [1]
- **70% of South Africans have fallen victim to cybercrime (vs. 50% globally)** [1]
- **Nigeria is simultaneously the largest target of and largest source of malicious internet activities** [1]
- **Estimated cost of cybercrime in Africa in 2016 was US$895 million** [2]

1. https://enachttps://enact-africa.s3.amazonaws.com/site/uploads/2017-09-26-enact-continental-report1.pdf
2. . http://serianu.com/downloads/AfricaCyberSecurityReport2016.pdf

Africa is under attack

Ransomware

Tunnels

Viruses

Remote Access Trojans

Cross-site scripting

Worms

Brute Force Attacks

PHISHING

Bots

Data Breaches

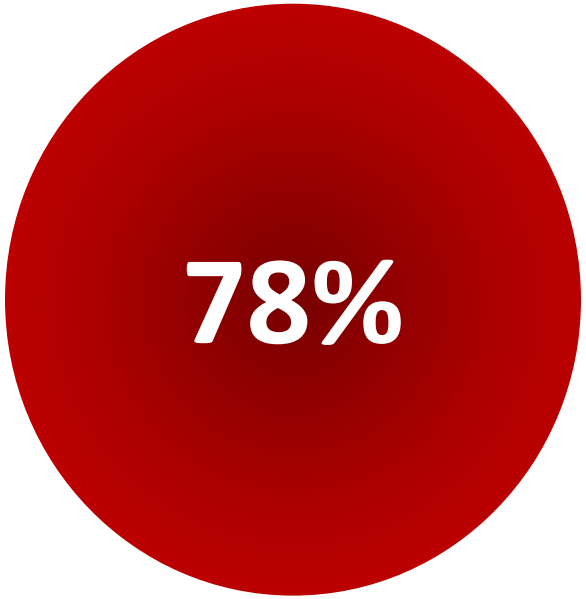
Advanced Persistent Threats

SQL Injections

Browser Attacks

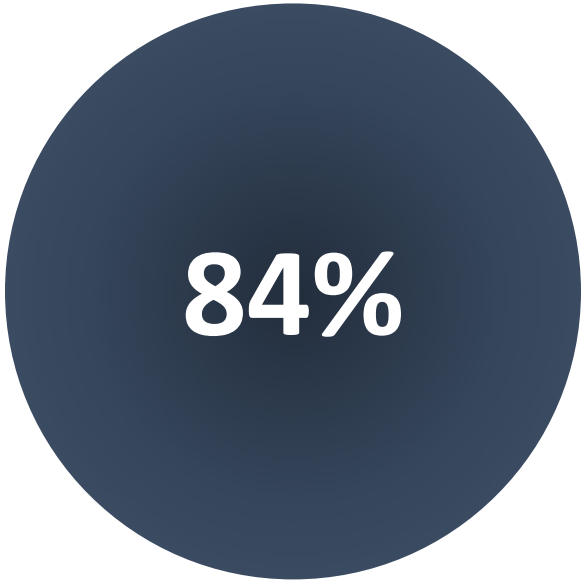
The Public DNS is Under Siege:

MOST ATTACKED



78% of attacks target the DNS, making it the #1 most attacked application layer protocol [1]

MOST ABUSED



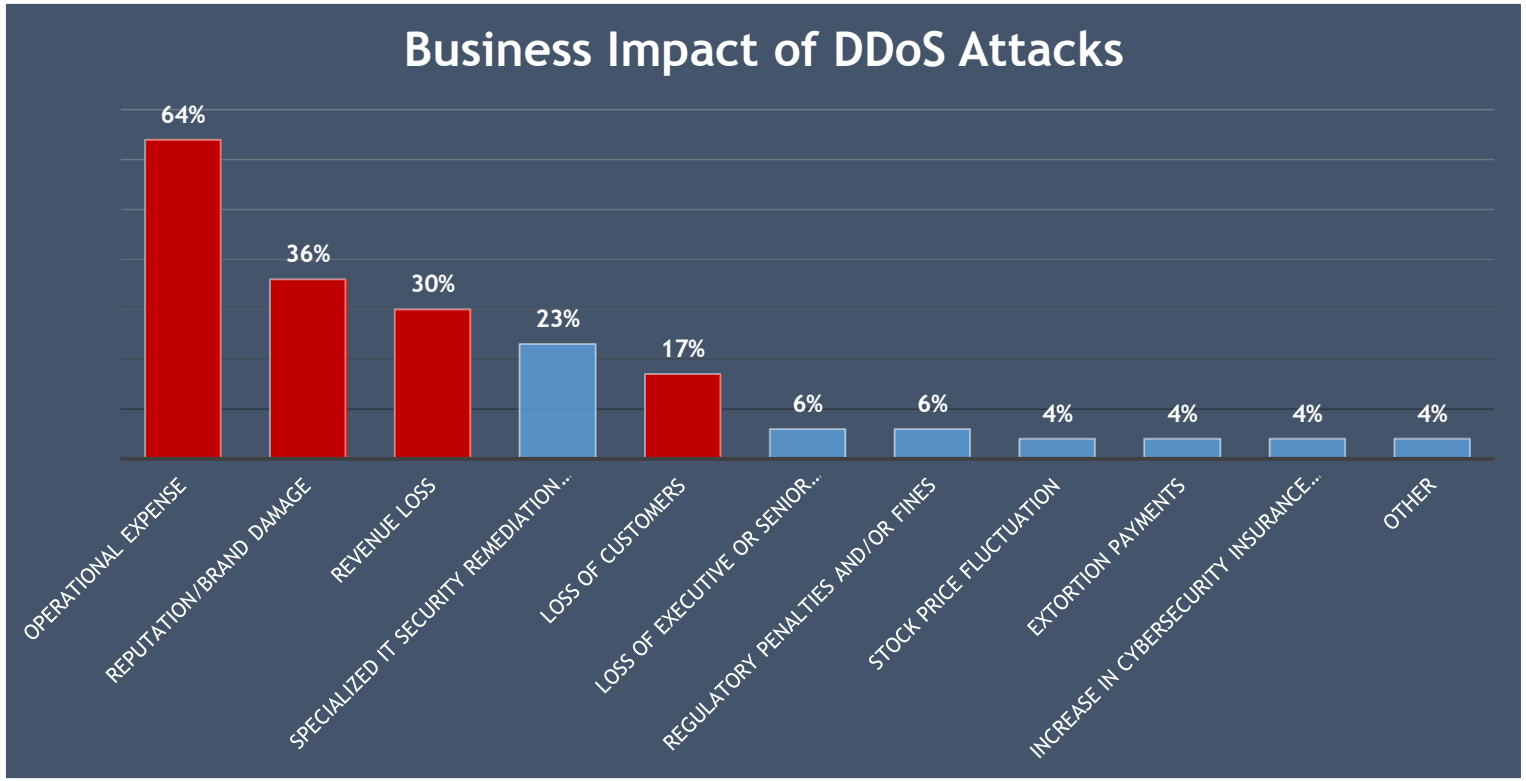
84% of reflected/amplified attacks use the DNS protocol to attack others [1]

MOST DIFFICULT TO PROTECT

50% of service providers report a customer-visible outage as a result of a DNS DDoS attack, despite protecting it with one or more traditional defenses [1]

1. Arbor Networks, 2015

The Cost of Cyber Crime – DDoS Attacks

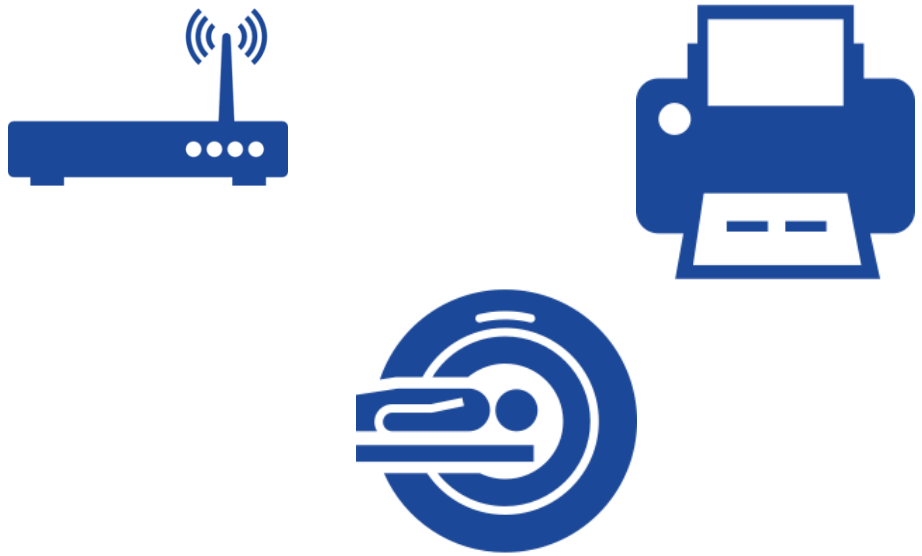


New Vector of Attack

IOT (Internet of Things)

IoT devices have little to no security and are hacked to join bot armies or as an entryway into networks

- MRI devices
- Industrial control systems
- Cars
- Remote cameras
- Printers
- Smart TVs
- Routers
- And thousands more….



…and use the DNS for Security

Modern bots & malicious software use the DNS

- Vast majority of bots now use the DNS to identify their C&C center
- Ransomware, phishing, trojans & other malware also use the DNS
- Fast flux and other techniques attempt to change DNS records more quickly

The DNS is then the ideal place to hunt and block bots, phishing and malware.

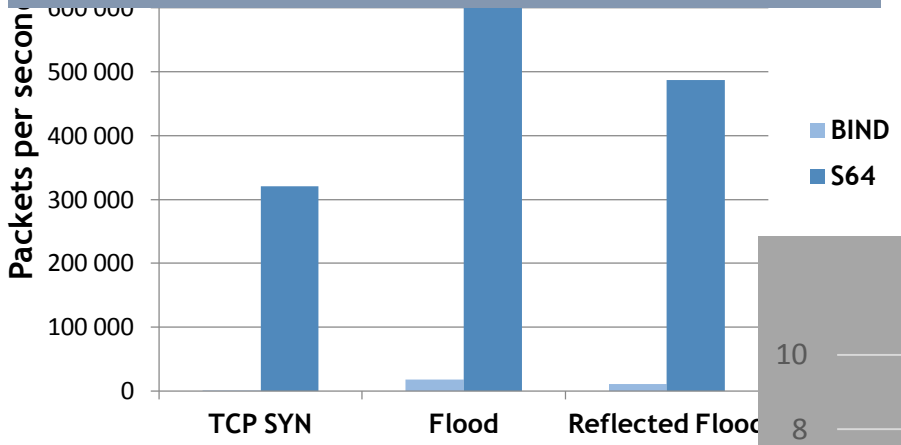
Secure the DNS…. Protect your Business

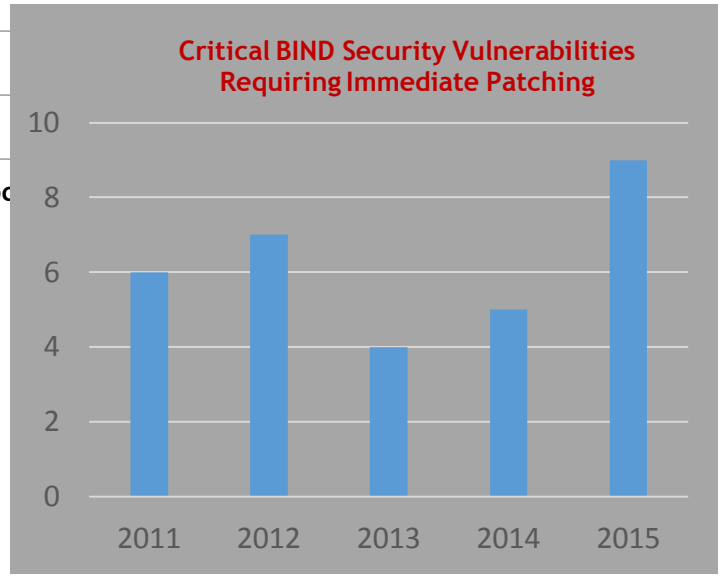
Be a trusted Service Provider for your Customers

- **Self-protecting servers that withstand high volume DDoS attacks**
- **Non BIND-based so not subject to BIND vulnerabilities**
- **Secure operating systems to prevent attacks on the server**

BIND DNS Has a Poor Security Track Record

Secure DNS solutions hardly impacted by attacks compare to BIND based DNS Solutions





Year	BIND	Secure64	Vulnerability ID	Impact
2016	🔴	🟢	CVE-2016-1284	Crash
	🔴	🟢	CVE-2016-1285	Crash
	🔴	🟢	CVE-2016-1286	Crash
	🔴	🟢	CVE-2016-2088	Crash
	🔴	🟢	CVE-2016-2775	Crash
	🔴	🟢	CVE-2016-2776	Crash
	🔴	🟢	CVE-2016-2848	Crash
	🔴	🟢	CVE-2016-6170	Crash
	🔴	🟢	CVE-2016-8864	Crash
2017	🔴	🟢	CVE-2017-3135	Crash
	🔴	🟢	CVE-2017-3136	Crash
	🔴	🟢	CVE-2017-3137	Crash
	🔴	🟢	CVE-2017-3138	Crash

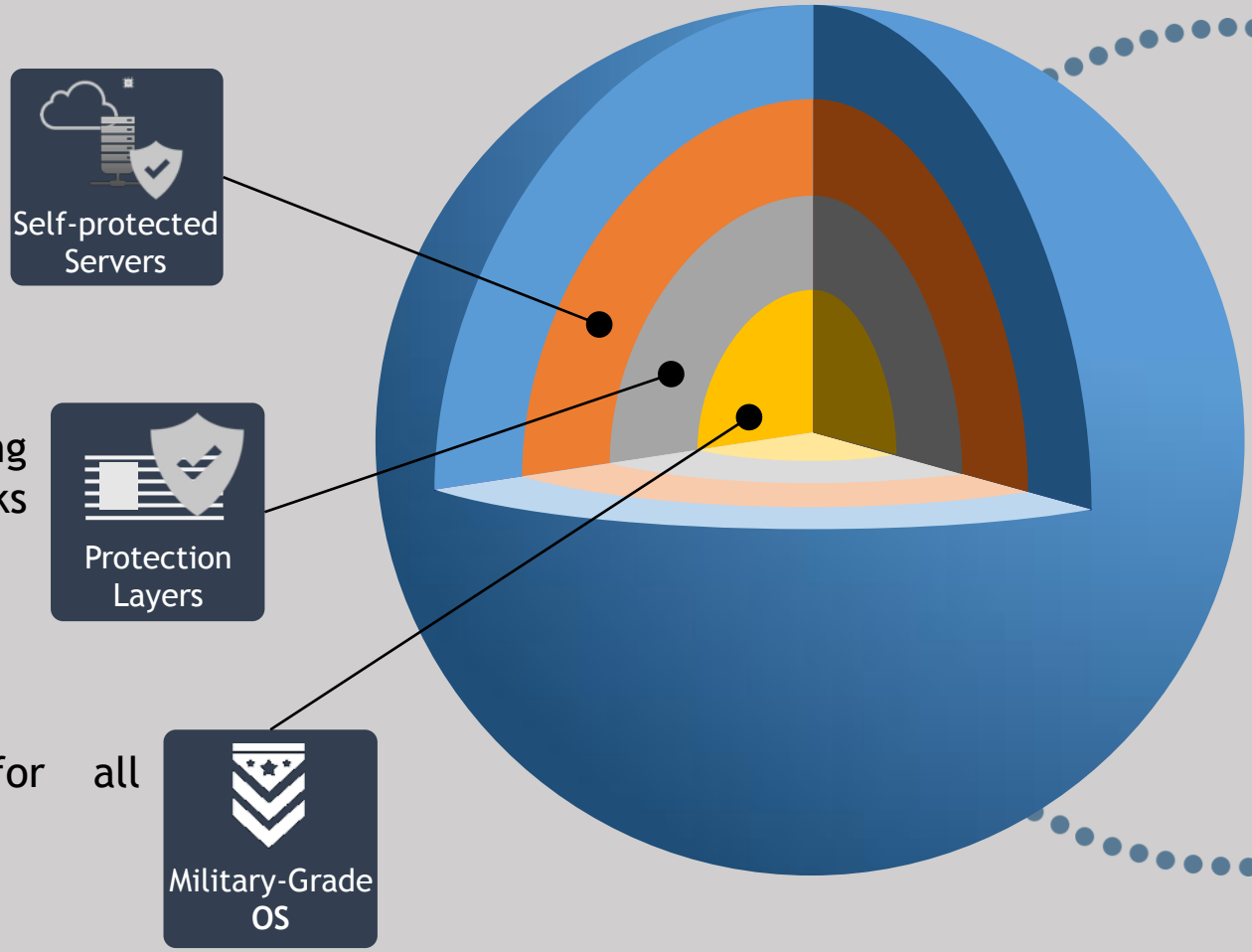
Generating Dramatic Business Impact!

The core of Secure DNS Security at Glance

Servers natively protected against any type of DDoS attacks. Six layers of protection to deliver carrier grade availability on DNS services.

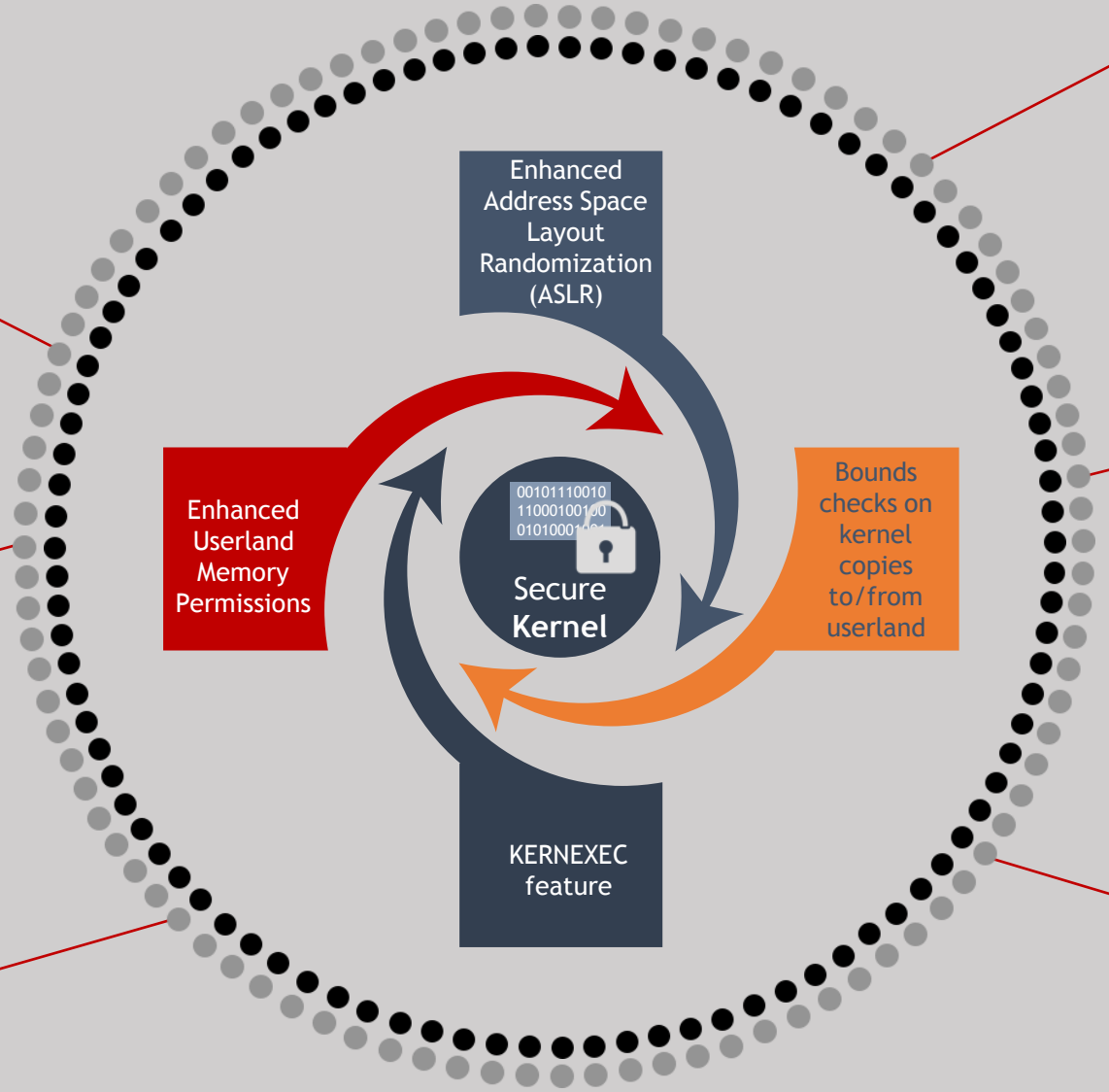
Highly efficient protection mechanisms ensuring clean traffic, allowing protection of both networks and end-users

Dedicated very secure operating system for all environments



Military Grade OS suite

Secure Kernel- Overview



Eliminates buffer overflow attacks

Prevents many privilege escalation attacks

Prevents modification of kernel objects

Protects against zero-day attacks

Prevents injected code from executing

Allows patching to be scheduled for a normal maintenance window

Some Secure DNS Key Differentiators

Instance Nationale des Telecommunications

1 Highly Scalable Carrier-Grade Secure DNS Platform

2 Unique Military-Grade **OS**

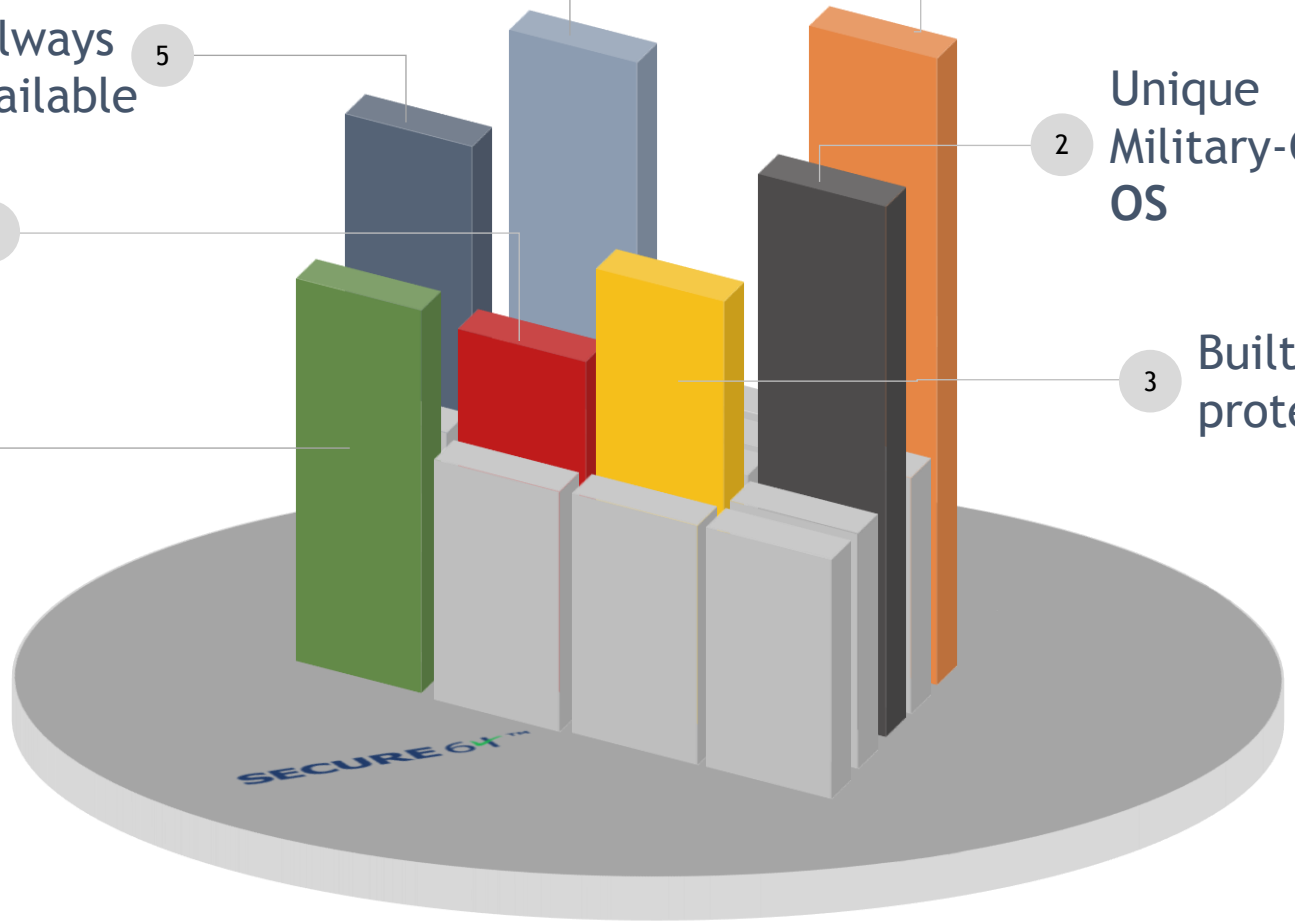
3 Built-in multi-layer DDoS protection

4 Not Based on BIND

5 Always Available

6 Lowest TCO & Best ROI

7 Best-In-Class Support



DDoS Attacks Can Destroy Your business in Minutes,

SECURE64™

Stop Them Before They Get In

Thank You for Being with us

GET Wireless – **A world of Competences**