

# Evolving Mobile Network Security Needs in the Age of IoT and 5G

SHARE THIS BROCHURE





Creating a Secure Climate  
for Your Customers

# Contents

- 00 Introduction
- 01 How Did We Get Here?
- 02 A New Atmosphere of Mobile Network Attacks
- 03 5G: New Capabilities, New Security Concerns
- 04 The Rise of IoT and 5G Devices
- 05 The Role of Security Automation and Artificial Intelligence
- 06 5G Security Use Solutions
- 07 Summary

Ever have that panicky feeling when you're not sure where you left your mobile device? It's a sign of the times that the sensation has a name: nomophobia.

*People simply hate to be disconnected. They want 24x7 access to high-speed internet everywhere from any device. All that tweeting, texting and telecommuting translates into dramatic growth in mobile traffic. Global mobile data usage is predicted to grow at a compound annual growth rate (CAGR) of 47%, reaching 49.0 exabytes per month by 2021. 📶*

Then factor in the internet of things (IoT), which includes billions of machines around the world connected to the internet. Every smart refrigerator, thermometer and printer, to name a few, require an always-on network connection for remote monitoring and data sharing.

While most service providers are just now getting a handle on 4G networks, 5G network trials 📶 are set to debut in major metropolitan areas in the United States by the end of 2018. The GSMA 📶 predicts Asia (China and Japan), Europe and the U.S. will be leading the 5G market by 2025.

*2020 is the beginning of a mass rollout of 5G networks. Service providers have a short runway to figure out security issues.*



These developments combine to create a complex mobile ecosystem with multiple entry points for attacks. Every device connected to your network is a potential security weakness.

Hackers can target your customers to steal data or use their devices to generate attacks on your network or other companies' networks and applications without the users' knowledge. IoT devices are especially vulnerable because manufacturers are more concerned with keeping prices low than adding security features. That means there are potentially millions of unprotected endpoints on your mobile network.

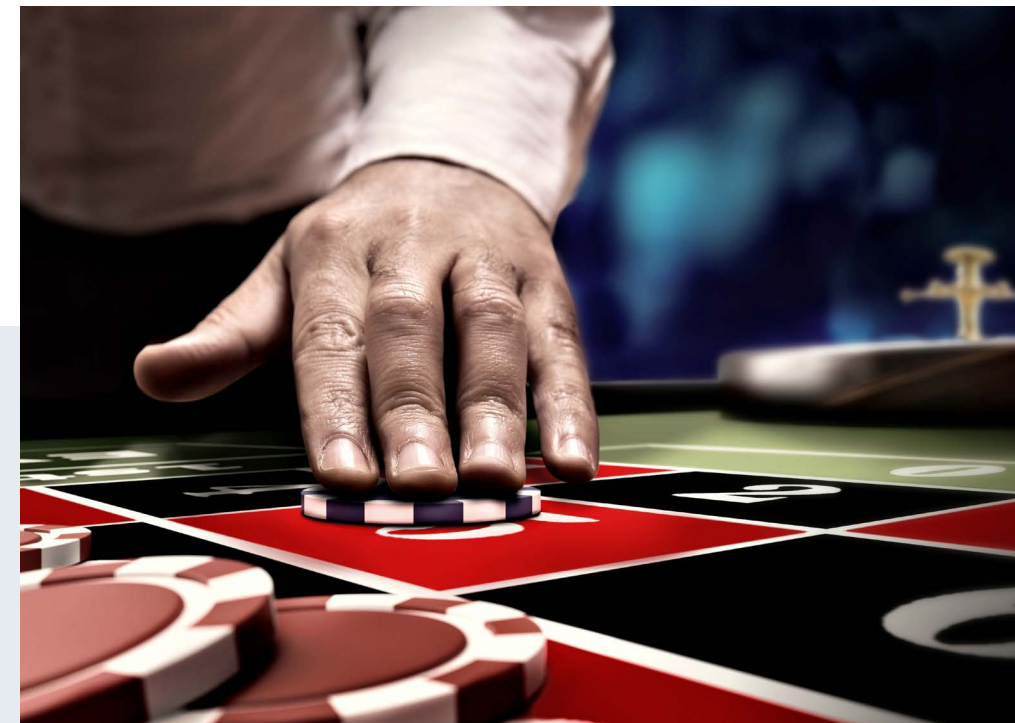
### THE CHALLENGE IS AN OPPORTUNITY.

**Mobile service providers can establish a competitive advantage by creating a secure environment that protects customers' data and devices, building superior trust with their users in comparison to other service providers.**

## SOMETHING'S FISHY HERE



**A CASINO FOUND OUT** the hard way that the internet of things is a jackpot for attackers. By tapping into the smart thermometer that controls the temperature of the water in the lobby aquarium, hackers went on a fishing expedition in the casino's network and landed its database of high-end clients.







# 01

---

How Did We Get Here?  
*The Evolving Network Security Environment*

➤➤ *The smartphones we take for granted have more computing power  than the computers that guided the Apollo 11 moon landing.*

In the almost quarter century since mobile devices transitioned from a luxury to a must-have, the severity of network security issues has kept pace. Network technologies tend to last 10 to 15 years before all users can be transitioned to the new network. That means

managing — and protecting — more network elements that are required as overlays and gateways to connect multiple generations of wireless devices. Each generation of network technology introduces a new set of security challenges.

## EVOLVING SECURITY CHALLENGES

*As mobile network technologies progress, new and more complex security issues are introduced. Service providers must adapt to protect their networks and create a secure online environment for customers.*

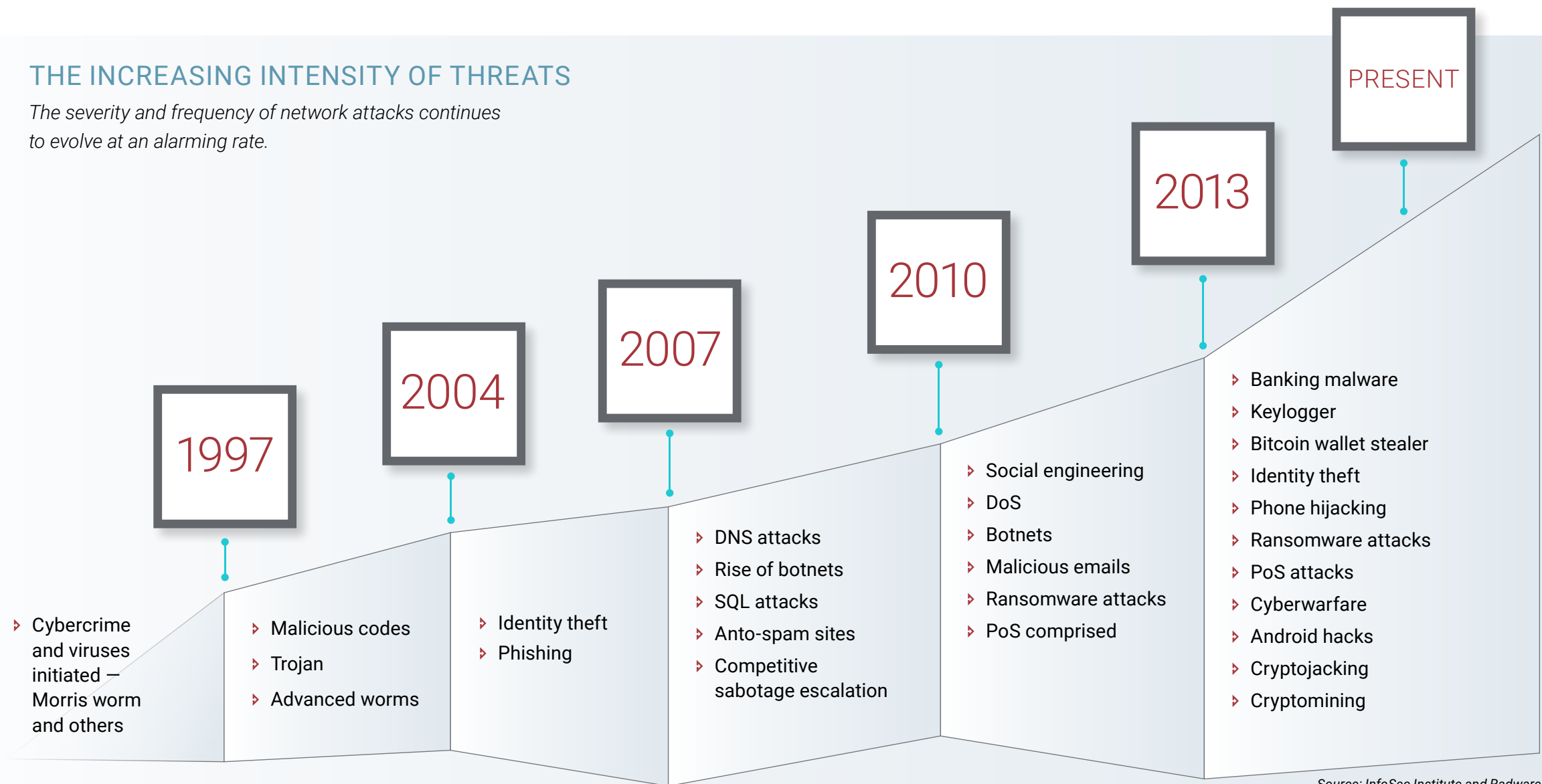
*5G connection speeds and latency are on par with wireline networks. The bad actors that threaten wireline networks will launch similar large-scale, complex attacks, which have been successful in wireline, on the 5G networks of unprepared service providers.*

Mobile Standard	Primary Focus	Typical DL Speed (Mbps)	Typical Latency (milliseconds)	Security Focus	Security Provisions
2G	Voice	0.1	629	Stealing voice calls	OTA encryption SIM cards
3G	Voice/data	8	212	Stealing data payload Rogue networks	Packet encryption Mutual authentication
4G	Data	15	96	Stealing data payload	Enhanced key management
5G	Data	~100	~1	<b>Mobile instantiated attacks</b> <b>Mobile security services</b>	<b>Cloud perimeter protection</b> <b>Secure network slices</b>



## THE INCREASING INTENSITY OF THREATS

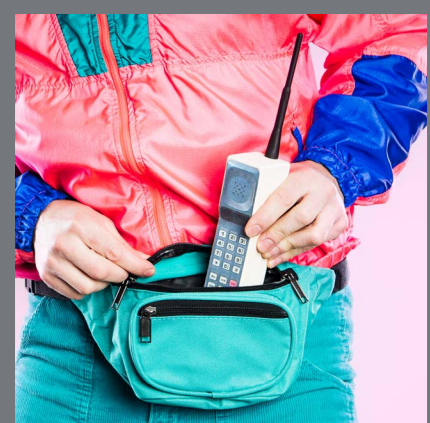
*The severity and frequency of network attacks continues to evolve at an alarming rate.*



Source: InfoSec Institute and Radware

Every generation of network technology introduces new threats to the mobile ecosystem.

2G



With the introduction of 2G in the 1990s, service providers' only concern is protecting voice calls. Security measures focus on authenticating and encrypting calls on the radio access link. Calls are not secured on the fixed network portion of the transmission.

3G



Faster speeds and access to the mobile internet are the hallmarks of 3G network technologies. The next generation of mobile networks offers much better security than 2G in the way it encrypts voice and data traffic. The main concern is not attacks on the network, but rather base station spoofing that enables hackers to listen in on data traffic.

WHY IS THE  
INTERNET  
NOT SECURE?



**PAUL VIXIE KNOWS.** The computer scientist who played a big role in the early days of the internet said that the system was intentionally built to be open. "Every app we built for the internet was designed as if it was for a boy in a plastic bubble, a completely clean environment with nothing malicious," Vixie said.

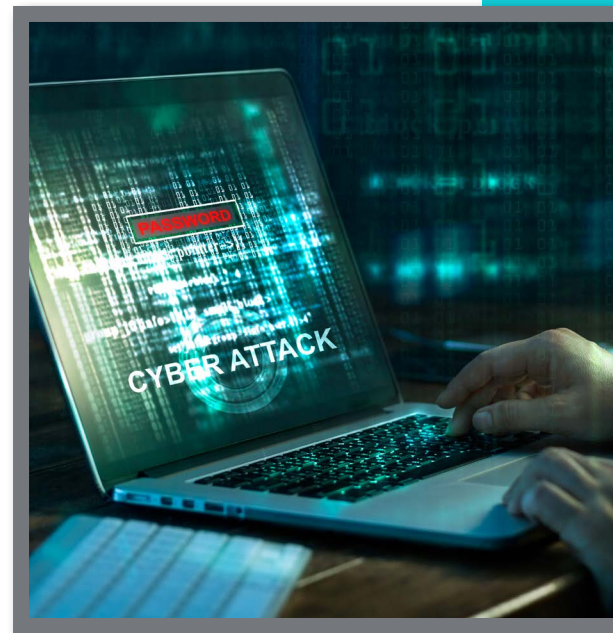


4G



The advent of 4G opens the mobile ecosystem and delivers significantly faster data speeds. But the security vulnerabilities in the 4G protocol enable attackers to impersonate devices to launch DDoS attacks or access users' sensitive data.

5G



5G mobile networks promise to be blazing fast with speeds similar to what's available on landlines. Users and IoT devices will greatly benefit from extremely low latency. All traffic is in the cloud; everything is distributed. On the flip side, the widespread rollout of next-generation networks is great for hackers because it broadens their ability to wreak havoc by attaching a server to a 5G connection from anywhere to team up with an army of other servers to launch attacks.

## ATTACK OF THE MOBILE DEVICES

**A NEW DISTURBING TREND IS EMERGING ON 4G NETWORKS.** In the past 12 months, hackers have figured out how to use mobile devices to launch network attacks. For example, a North American service provider noticed a slowdown in mobile traffic which the provider originally blamed on congestion. With the help of Radware, further investigation revealed that about 30% of the traffic on the wireless network came from mobile devices launching DDoS attacks without the users' knowledge.





# 02

A New Atmosphere of  
Mobile Network Attacks



## ➤ ➤ *The climate for mobile network attacks is constantly changing.*

It's difficult for network security managers to forecast and prepare for what's next because hackers never sit still. They're always developing new and technologically sophisticated ways to target mobile network services and their customers. Watchdog groups have taken notice and are raising alarms on the preparedness of service providers to mitigate attacks on 5G networks.

A Federal Communications Commission (FCC) advisory group [recently warned](#) 🕸️ that 4G mobile networks are “increasingly vulnerable to cyber intrusion” because of threats to the Diameter protocol, a weak link in mobile networks that enables outside traffic to flow between operators' networks. While no real attacks are reported, some suspect traffic has been detected.

Cybersecurity agency ENISA [warns that](#) 🕸️, as 5G is rolled out, unless development of standards keeps pace, security risks prevalent in current mobile technologies will carry forward.

Because 5G network operators want incremental opportunities to monetize the network and applications, more cloud applications will be dependent on a variety of APIs. That gives rise to a complex world of interconnected devices, including smartphones, mobile devices and IoT appliances. Hackers will be able to exploit a single point of access in a cloud application to quickly expand the attack radius to other connected devices and applications.

### ARMY OF DIGITAL ATTACKERS

One hacker can quickly become an army of attackers by deploying botnets, a series of computers or mobile devices infected with malware that enables them to be directed remotely by a command and control (C&C) service or internet relay chat (IRC). The collective computing power of a botnet, such as the Mirai botnet, can generate DDoS attacks large enough to shut down major websites.

Botnets are difficult to halt because so many devices that are not secure are connected to the internet. The dramatic growth of internet of things (IoT) devices increases the number of vulnerable endpoints. [Gartner estimates](#) 🕸️ that, by 2020, there will be 20.4 billion connected devices.

Many hackers rent access to botnets for others to exploit. [For example](#) 🕸️, a group called Los Calvos de San Calvicio offers a DDoS attack of about 300 Gbps for only \$20 per target. DDoS-for-hire services make it easy for anyone with malicious intent to launch an attack — whether they have technical savvy or not. The world's biggest DDoS-for-hire “webstressor.org” service was [recently shut down](#) 🕸️ by the United Kingdom's National Crime Agency (NCA) and Dutch police, but it likely won't take long for new services to pop up.

EVOLVING THREATS

Mobile service providers face a variety of known and developing threats targeting their networks.

Attack Types	Description	Additional Information
Application attacks	Attacks target the application layer (Layer 7) of the network. Low and slow DDoS attacks mimic legitimate traffic to wear down network resources.	<a href="#">What to look out for in application attacks</a>
Burst attacks	These repeated short bursts of high-volume attacks at random intervals are also known as hit-and-run DDoS. Each short burst can last only a few seconds, while a burst attack campaign can span hours or even days and unleash hundreds of gigabits per second of throughput toward its target.	<a href="#">Are you protected against burst attacks?</a>
DNS attacks	Attackers take advantage of vulnerabilities in domain name servers (DNS) to overwhelm the servers with IP address verification requests.	<a href="#">Top 10 DNS attack types</a>
Encrypted attacks	The percentage of encrypted traffic on networks is rising considerably, but most companies do not decrypt SSL traffic and are blind to whether the payload is good or bad.	<a href="#">More than 35% of cyberassaults leverage SSL-based attack vectors</a>
iOS malware	The iOS on Apple products is rigid, but iPhone users can rest easy no longer. Hackers are up to the challenge to infect iOS devices with malware.	<a href="#">Report finds rate of iOS malware increasing faster than Android malware</a>
IoT attacks	Billions of IoT devices are already in use and continue to grow in popularity. Each device represents an unsecured endpoint that hackers can exploit to launch massive attacks.	<a href="#">Five nightmarish IoT attacks</a>
Smartphone infections	Android smartphones are the most popular target for mobile malware because the open operating system is easier to manipulate. Infections are spread by email or embedded in apps and mobile websites.	<a href="#">Malware infection rate on Android devices is soaring</a>





### IMPACT ON MOBILE SERVICE PROVIDERS

When attacks happen, enterprises and individual users may at first experience issues with latency or service availability. Performance issues will be blamed on the mobile service provider. Large-scale attacks can take down the network for an extended period of time. Your reputation is at risk.

In the fall of 2016, a DDoS attack on DNS provider Dyn took down many internet services in Europe and North America, such as CNN, PayPal and Walgreens. Internet-connected devices carrying Mirai malware formed the botnet. Dyn estimated that the attack had involved 100,000 malicious endpoints, and the company, which is still investigating the attack, said there had been reports of an extraordinary attack strength of 1.2 Tbps.

The source code for Mirai malware is public and easily manipulated. Anyone can use it. As the number of IoT devices continues to grow, expect more attacks of this type. Is your network prepared to secure endpoints?

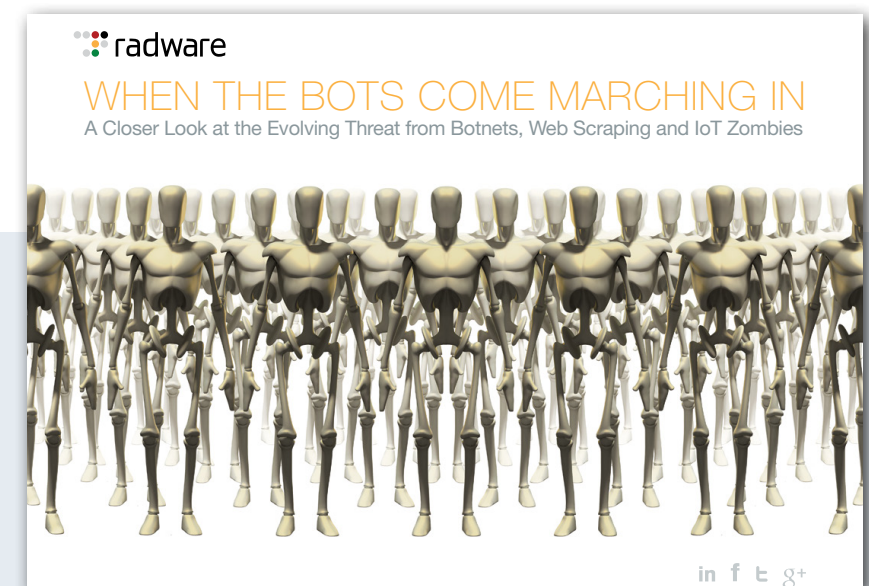
Most mobile device users assume apps downloaded from the internet have been vetted for safety. Apple and Google do have strong safeguards in place, but hackers still find ways to slip malicious malware into free downloads. Android devices are more vulnerable because the operating system is open. In August 2017, the [WireX](#) botnet network infected more than 120,000 Android smartphones. Users downloaded more than 300 apps from the Google Play store that contained malicious malware designed to launch massive application layer DDoS attacks.

### GET A CLOSER LOOK AT THE EVOLVING THREAT FROM BOTNETS

**BAD BOTS** — including those that exploit internet of things (IoT) devices as weapons of attack — are one of the fastest-growing and changing threats in the security landscape. Learn more about why bots are so powerful and how to become a “botnet killer” in the [When the Bots Come Marching In](#) white paper.

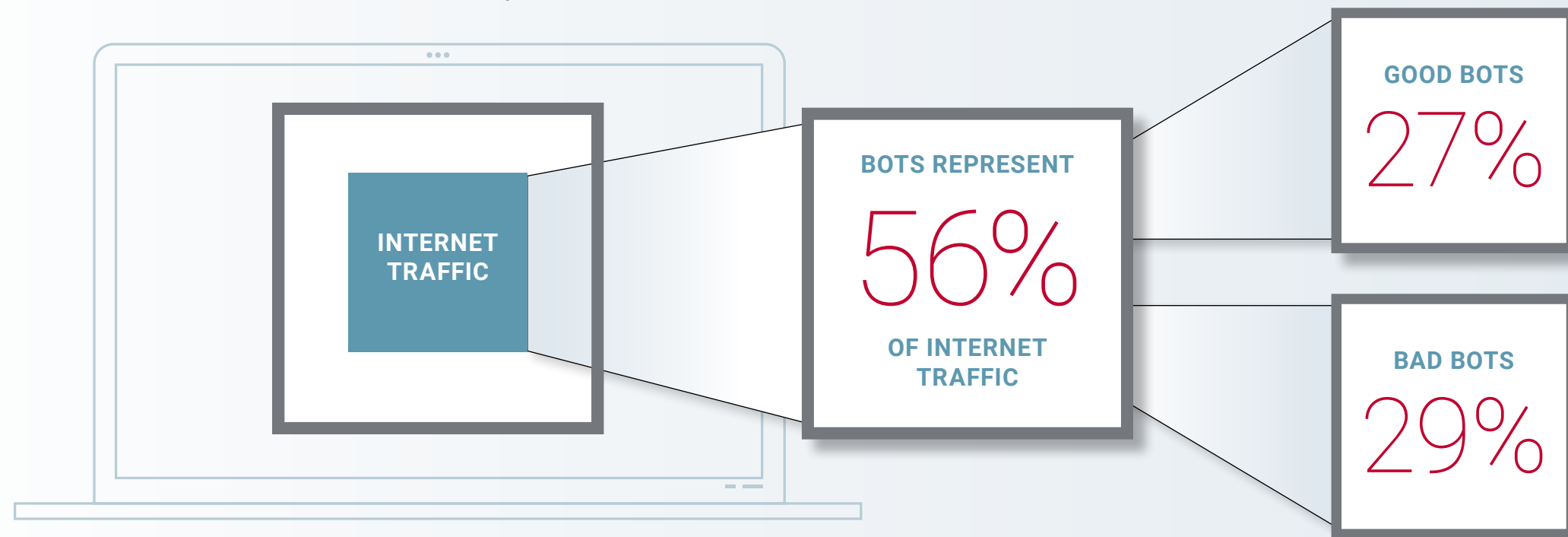
Dyn estimated that the attack had involved “100,000 malicious endpoints.”

The Guardian



### BOTS ARE BIG PLAYERS IN THE ONLINE WORLD

*Almost one-third of bot traffic on the internet is designed to cause harm.*



### SEPARATING THE GOOD FROM THE BAD

It would be nice if all attacks looked like bad traffic. The problem is many attackers use legitimate traffic to launch attacks that overload websites and mission-critical applications or infrastructures.

It is imperative that a mobile network security solution is able to differentiate attacks carried on networks from legitimate traffic and stop them before they cause harm to the network or other users.

Not all bot traffic is bad. Bots account for 56% of internet traffic. Almost half of that bot traffic is for positive purposes. Bots routinely scrape the internet to gather information for search engines, look for intellectual property and discover copyright violations among other useful tasks.

Bad bot traffic is used for attacks on networks, servers, smartphones and connected devices to cause damage through DDoS, steal data, exploit intellectual property and purge inventory in online shops and ticketing systems.



## WHO ARE THE ATTACKERS?

**RICHARD CLARKE**, former special cybersecurity adviser to the U.S. president, devised an acronym — CHEW — to categorize and explain the origin of cyberattacks threatening mobile operators, carriers and enterprises.

- ▶ **Crime (cyber)** — the notion that someone is going to attack you with the primary motive being financial gain from the endeavor.
- ▶ **Hacktivism** — attacks motivated by ideological differences. The primary focus of these attacks is not financial gain but rather persuading or dissuading certain actions or “voices.”
- ▶ **Espionage** — straightforward motive of gaining information on another organization in pursuit of political, financial, capitalistic, market share or some other form of leverage.
- ▶ **War (cyber)** — the notion of a nation-state or transnational threat to an adversary’s centers of power via a cyberattack. Attacks could focus on nonmilitary critical infrastructure.

The attackers can range from a tech-savvy teenager to a highly organized group that taps into huge server farms in places like Russia and Ukraine to facilitate attacks.

According to a Ponemon Institute study:

### *The Internet of Things (IoT) — A New Era of Third-Party Risk*

*While the threat of attacks on IoT devices is well-known, little is being done to prepare for the onslaught. Service providers have an opportunity to take the lead.*

81%

think an IoT data  
breach is likely in the  
next two years

97%

believe IoT devices  
could wreak havoc on  
their organizations

29%

(less than 1/3)  
monitor for IoT risks  
to their networks






# 03

5G: New Capabilities,  
New Security Concerns



## ➤➤ In December 2017, the Third Generation Partnership Project (3GPP) moved forward the 5G Phase 1 system architecture .

With the approval of the first set of 5G new radio (NR) specs, it's a significant milestone on the path to commercial 5G rollouts. While 4G is expected to **dominate the market**  through 2025, with the faster speeds and lower latencies promised by 5G, demand for services will begin as soon as 2020.

Within the time frame, mobile service providers have a runway in which to prepare for the new security risks that are inherent in 5G networks.

### WHAT'S DRIVING THE MOVE TO 5G?


5G is the next generation of mobile internet connectivity that offers:

- 100x faster transmission speeds, which improve network performance
- Lower latency, which improves device connections and application delivery
- 1,000x greater data capacity, which better supports more simultaneous device connections
- Better user experience through value-added services enabled by network slicing

These factors combine to propel the growth of the mobile internet for enterprise and individual use, as well as the explosion of connected internet of things (IoT) devices.

Unlike previous generations of mobile network technologies, the architecture of 5G is distributed. All network elements and operations move to the cloud. There's no longer a need for dedicated fronthaul or backhaul, a transport layer or central office connectivity.

### 5G TERMINOLOGY

**5G INTRODUCES** more than just faster speeds and lower latency. Here's a **list of definitions**  to help keep you up to speed on all the new terminology.

#### THE CHALLENGES OF A SOFTWARE-BASED, DISTRIBUTED NETWORK ARCHITECTURE


Because of its distributed nature, the implementation and deployment of 5G networking infrastructures will change dramatically. Software-defined networking (SDN) and network function virtualization (NFV) will flatten the radio access network (RAN) as well as the evolved packet core (EPC) and reduce power requirements for data transmission.

Services can be flexibly allocated anywhere on 5G networks, including network nodes, end-user devices or external hosts. That means services are not necessarily confined to service providers' networks and can originate from outside the network domain.

The benefit is that services can be placed on virtualized network functions on resources that are physically close to users and IoT devices for faster, more efficient delivery, but the distributed nature of 5G networks introduces a number of new security challenges.



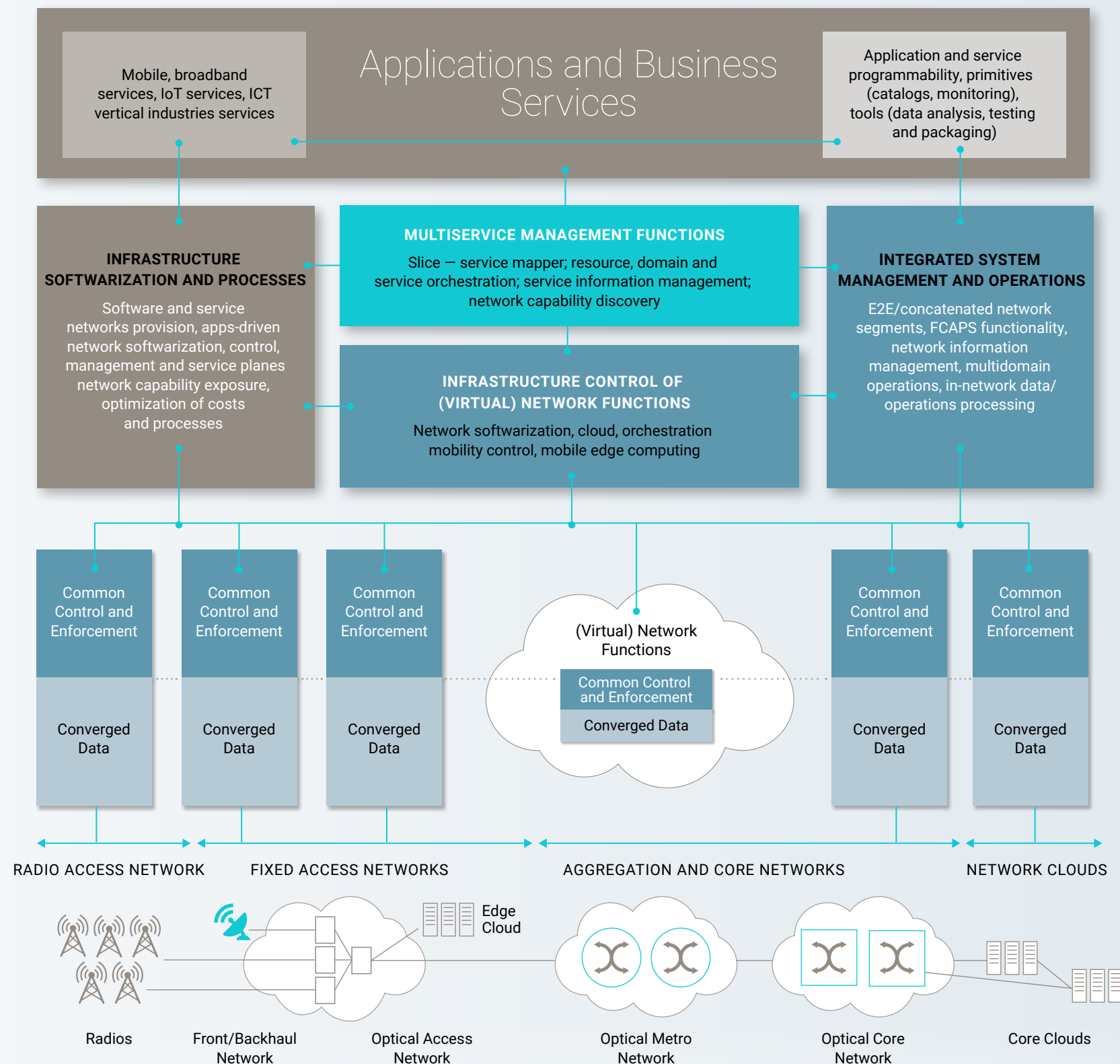
*"5G networks are much more likely to be networks of small cells, even down to the size of home routers, than to be huge towers radiating great distances. Some of that is because of the nature of the frequencies used, but a lot of that is to expand network capacity. The more cells you have, the more data you can get into the network."*

"What Is 5G?," PC Magazine 



## NETWORK SOFTWARIZATION AND PROGRAMMABILITY FRAMEWORK

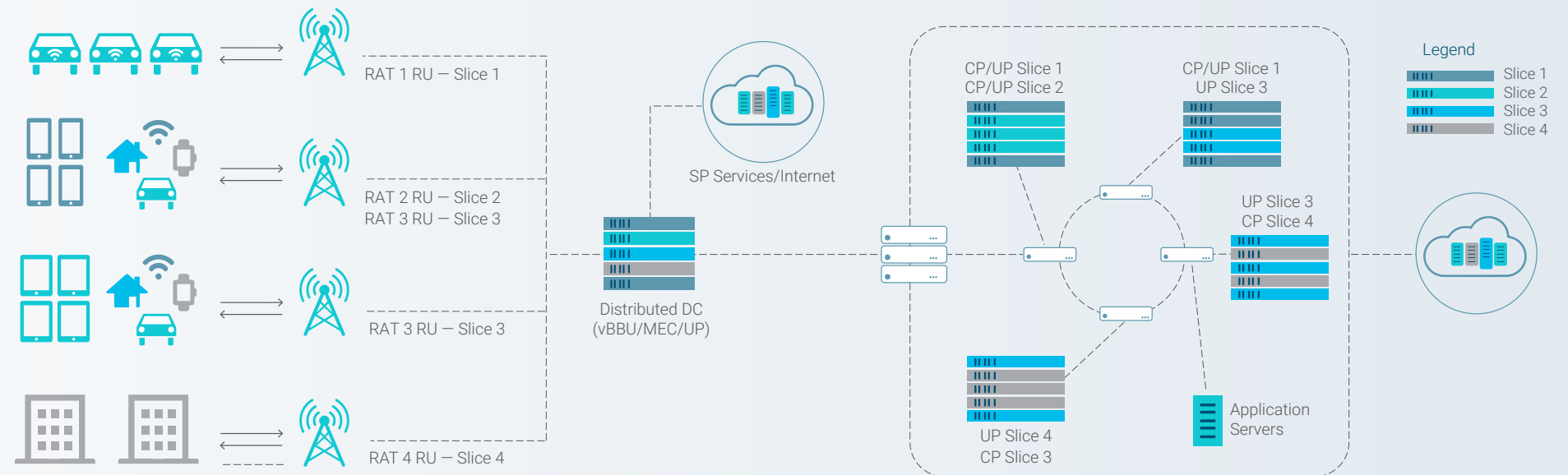
According to the 5G-PPP Architecture Working Group's [View on 5G Architecture](#) paper, "5G networks enable the uniform management and control of operations that are becoming part of the dynamic design of software architectures. The network 'softwarization' and programmability are part of the basis for the 5G architecture design."



Source: 5G PPP, View on 5G Architecture

## 5G ARCHITECTURE DISTRIBUTES THREATS THROUGHOUT THE NETWORK

According to Cisco, the 5G network expands the threat surface for attacks because the network architecture is more flexible and open to the internet. For localization and to reduce latency, applications and use cases need compute and storage locations closer to the edge of the network. Virtualized components are placed across distributed edge and centralized core clouds. There is an emphasis on software-based network enablers such as SDN (software-defined networking), SDA (software-defined access) and SDR (software-defined radio).



### DEVICE THREATS

Malware  
Sensor susceptibility  
TFTP MitM attacks  
Bots DDoS  
Firmware hacks  
Device tampering

### AIR INTERFACE THREATS

MitM attack  
Jamming

### RAN THREATS

MEC server vulnerability  
Rogue nodes

### BACKHAUL THREATS

DDoS attacks  
CP/UP sniffing  
MEC backhaul sniff

### 5G PACKET CORE AND OAM THREATS

Virtualization  
Network slice security  
API vulnerabilities  
IoT core integration  
Roaming partner vulnerabilities  
DDoS and DoS attacks  
Improper access control

### SGI/N6 AND EXTERNAL ROAMING THREATS


IoT core integration  
VAS integration  
App server vulnerabilities  
Application vulnerabilities  
API vulnerabilities

## THE 5G ARCHITECTURE

An SDN/NFV-supported foundation transitions 5G services and technologies to the cloud. The 5G architecture separates the user data and control planes, which improves network flexibility and centralized control and makes performing network slicing easier.


### Open and Virtual

The nature of 5G networks requires an open ecosystem. Unlike earlier generations of networks that are controlled by the service provider that owns and manages the infrastructure, 5G depends on the virtualization of network functions. The result for service providers is less control over the physical elements of the network.

According to Ericsson,  "For the same reason, standard interfaces to the computing/network platforms – such as those defined by ETSI (the European Telecommunications Standards Institute) in their network function virtualization work – are necessary to ensure a manageable approach to security. When operators host third-party applications in their telecom clouds, executing on the same hardware as native telecom services, there are increased demands on virtualization with strong isolation properties."

NFV and its sister technology, software-defined networking (SDN), are mainstays of the 5G cloud-based architecture. The application stacks riding in the cloud environment enabled by SDN and NFV technologies introduce new threat vectors.



Vulnerabilities in software components are a major challenge to securing the NFV environment. **Nokia**  warns that, for example, “when applying NFV, the integrity of virtual network functions (VNFs) and the confidentiality of their data may depend to a larger degree on the isolation properties of a hypervisor. More generally, they will also depend on the whole cloud software stack.”

Attacks on SDN control applications that interact with a central network controller can also cause major issues for mobile service providers.

#### Network Slicing


5G enables service providers to “slice” portions of a spectrum to offer specialized services for specific types of devices. Different slices can be associated with security, data-flow isolation, quality of service, reliability and other important factors. The technique of network slicing enables the definition of multiple logical network slices on top of the same physical infrastructure.

Resources can be dedicated exclusively to a single slice or shared between different slices. A network slice may also support one or many services. It can be used to create a virtual operator network for several purposes, including a complete private network, a copy of a public network to test a new service or a dedicated network for a specific service.

Because most network functions will operate in NFV environments, NFV security considerations greatly impact 5G mobile network security architectures. Security measures that separate different network slices running on the same infrastructure are necessary to secure data and prevent virtual machines in one slice from communicating with other slices. When network functions are no longer assigned to specific hardware elements, dynamic software allocation plays a big role in security protocols.

#### SECURITY FOCUS AREAS

As 5G rolls out, mobile service providers face a number of new security issues to protect their customers’ applications and data.

**Nokia**  points out that “. . . 5G networks must support a very high level of security and privacy for their users (not restricted to humans) and their traffic. At the same time, networks must be highly resistant to all kinds of cyberattacks. To address this twofold challenge, security cannot be regarded as an add-on only; instead, security must be considered as part of the overall architecture and built into the architecture right from the start.”

5G networks introduce a new level of security considerations because services are virtualized.

Enterprises will increasingly look to service providers to offer proof of how their 5G networks are secured before committing to services.





# 04

---

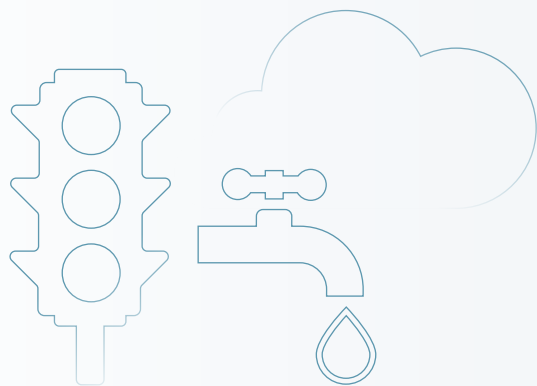
The Rise of IoT  
and 5G Devices



➤ The architecture of 5G networks is ideally suited for IoT devices that require low latency and fast data transmission, and its huge capacity is able to manage large numbers of concurrent device connections.

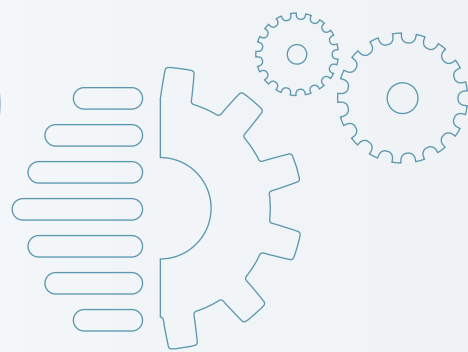
### GARTNER POINTS 🚫 TO 20.4 BILLION IOT "THINGS" BY 2020.

*IoT devices will show up in just about every aspect of daily life. While IoT devices promise benefits such as improved productivity, longevity and enjoyment, they also open a Pandora's box of security issues for mobile service providers.*



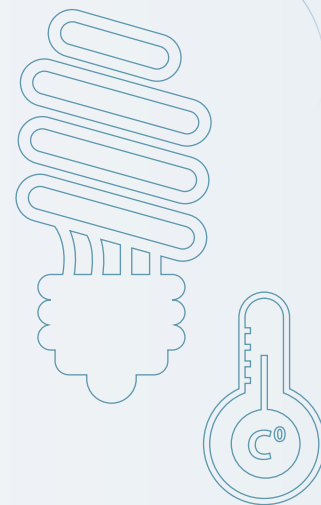
#### SMART CITIES

Traffic control, power plants, community services, water supply



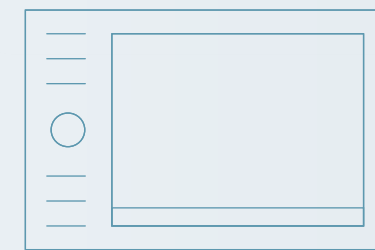
#### SMART BUSINESSES

Office equipment, manufacturing equipment, telemetry



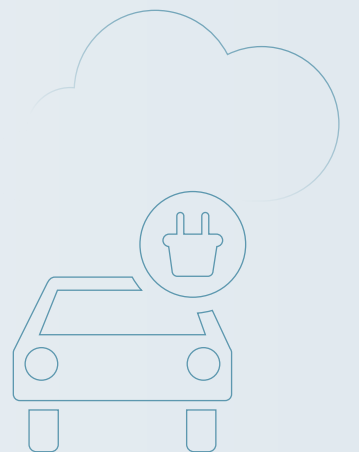
#### SMART BUILDINGS

Heating, air conditioning, security, utilities



#### SMART HOMES


Kitchen appliances, heating, air conditioning, security, entertainment devices



#### SMART CARS

Self-driving, system diagnostics, monitoring

## IOT DEVICES ARE RIPE FOR ATTACK

As connectivity and services move to the cloud, attackers target IoT devices for [a number of important reasons](#): 

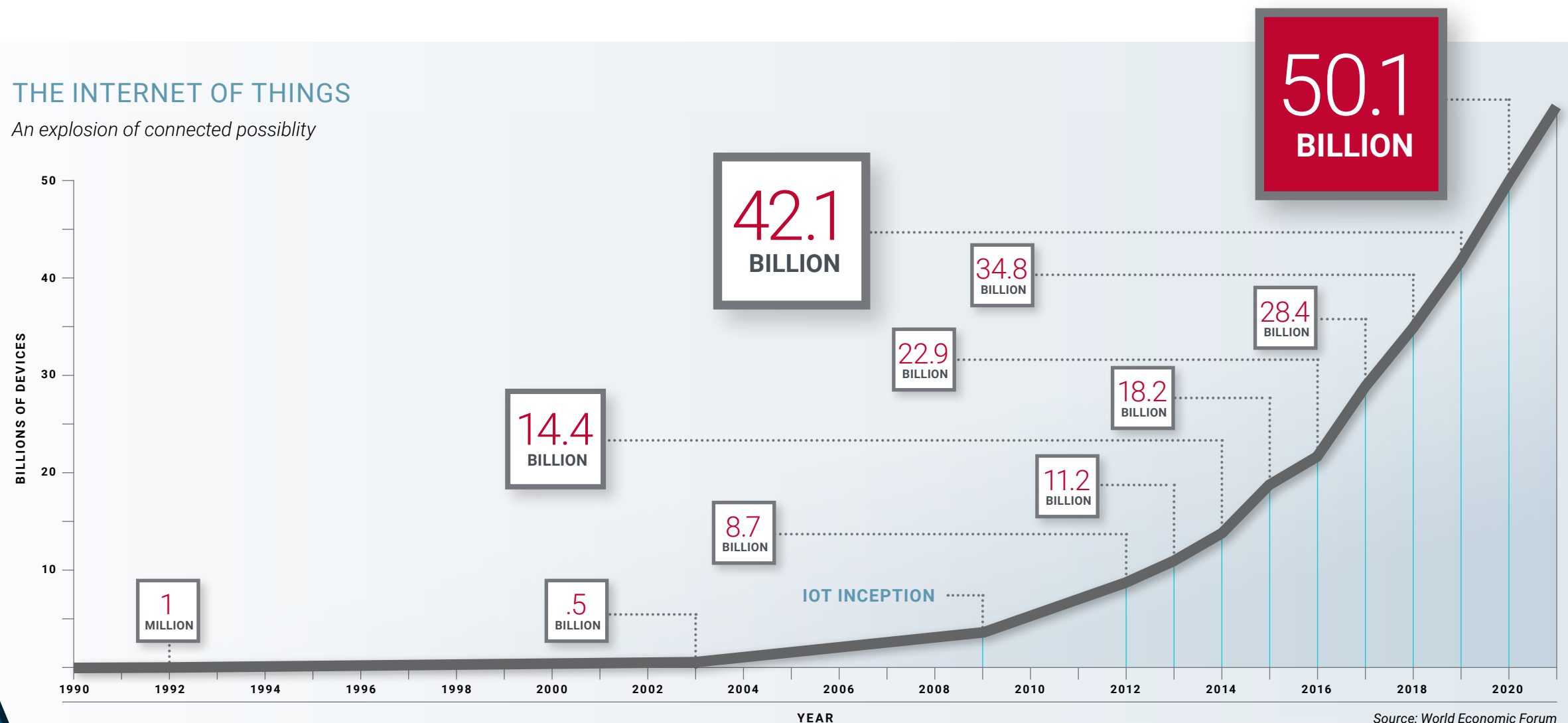
- ▶ Embedded devices are easily exploitable (e.g., using default credentials or exposed services).
- ▶ Always-on devices are available 24x7x365.
- ▶ Off-the-shelf products typically have low security standards. They often use obvious and documented credentials for CLI access, which cannot be changed through an admin GUI, run exposed services as root, do not encrypt user passwords and fail to provide authentication for “remove configuration” services.

- ▶ Malware leverages security controls (iptables, port filters) and kills service processes to prevent users from logging in or competing bots from taking control.
- ▶ IoT devices are rarely monitored and poorly maintained, which makes it easy for hackers to shut down or enslave large numbers of devices.
- ▶ Hackers can achieve control of thousands of devices for little to no cost. By contrast, they face high costs when accessing and controlling servers for more traditional DDoS attacks.

All of these new devices create a threat landscape that requires mobile service providers to change their approach to network security or suffer the consequences. The same old tools are no longer good enough.

## THE INTERNET OF THINGS

*An explosion of connected possibility*





### WHO OWNS THE PROBLEM?

Unfortunately, the answer to this question right now is no one.

**Device Manufacturers:** IoT device manufacturers are focused on delivering solutions customers want at the lowest possible cost. Margins are the priority. There's little regulatory control or oversight. Security features add development time and costs. Plus the ever-changing scope of attack types makes it impossible for manufacturers to address every possibility.

**Component/Software Developers:** Upstream manufacturers producing components and/or software can cause problems across hundreds of brands and devices. Security flaws can be exploited across any downstream device manufacturer that uses them.

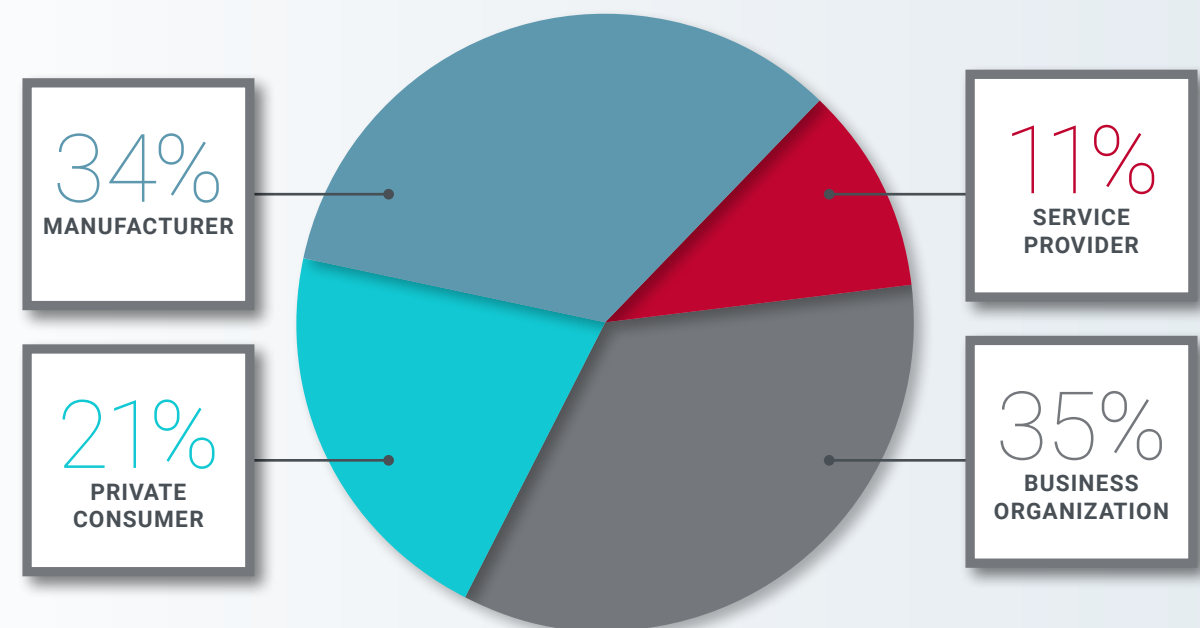
**Enterprises:** There's simply no way for IT departments to keep up with the explosion of connected devices that will hit their networks over the next decade. Even with strict use of endpoint protection solutions and policies about what types of applications and devices are permitted, all it takes is one weak link. According to a [Radware survey of C-suite executives](#), more than half of respondents want service providers to offer network security support.

**Service Providers:** The emergence of 5G is the launch of the true mobile internet. While service providers don't own the emerging security issues, it is ultimately up to the operators to deal with and mitigate attack traffic.



### WHO IS ACCOUNTABLE FOR RISKS POSED BY IOT DEVICES AS HUBS?

*There is no clear agreement on what entity is responsible for securing IoT devices, according to a recent cross-industry survey.*



Source: Radware's "Global Application & Network Security Report, 2017-2018"

### IOT INCIDENTS IN THE NEWS

**ATTACKS ON IOT** can turn everyday items into threats worthy of a science fiction movie. Check out [The 7 Craziest IoT Device Hacks](#) in recent years.





# 05

## The Role of Security Automation and Artificial Intelligence



➤➤ *As threats grow more complex, innovation is needed in response to detect attacks before they cause harm.*

Security threats and anomalies within network traffic are growing faster than security teams can detect and react to them. The growing storm of data that travels networks is actually making it harder to detect threats. Automation is key to better identification and mitigation of threats.

Currently, traditional machine-learning tools enable real-time detection and mitigation of DDoS attacks. Through behavioral analysis, bad traffic is identified and automatically blocked before it causes harm.

All the security threats we see now on enterprise networks are a harbinger of what's to come on 5G networks. The introduction of 5G adds significant complexities to mobile networks that require additional security measures. Added bandwidth and decentralized controls make every device with an IP address that is connected to the internet a possible launching site for malicious attacks.

#### THE NETWORK AS A SENSOR

In 5G networks, network elements are distributed at the edge and virtualized. Now all the endpoints throughout the network can be used as detection spots to send messages back to a centralized control plane. Think of the network as one big sensor.

The centralized control plane serves as the brain of the network, compiling all the inputs from its telemetry feeds to figure out the best way to apply mitigation policies.

PUTTING BIG DATA TO WORK

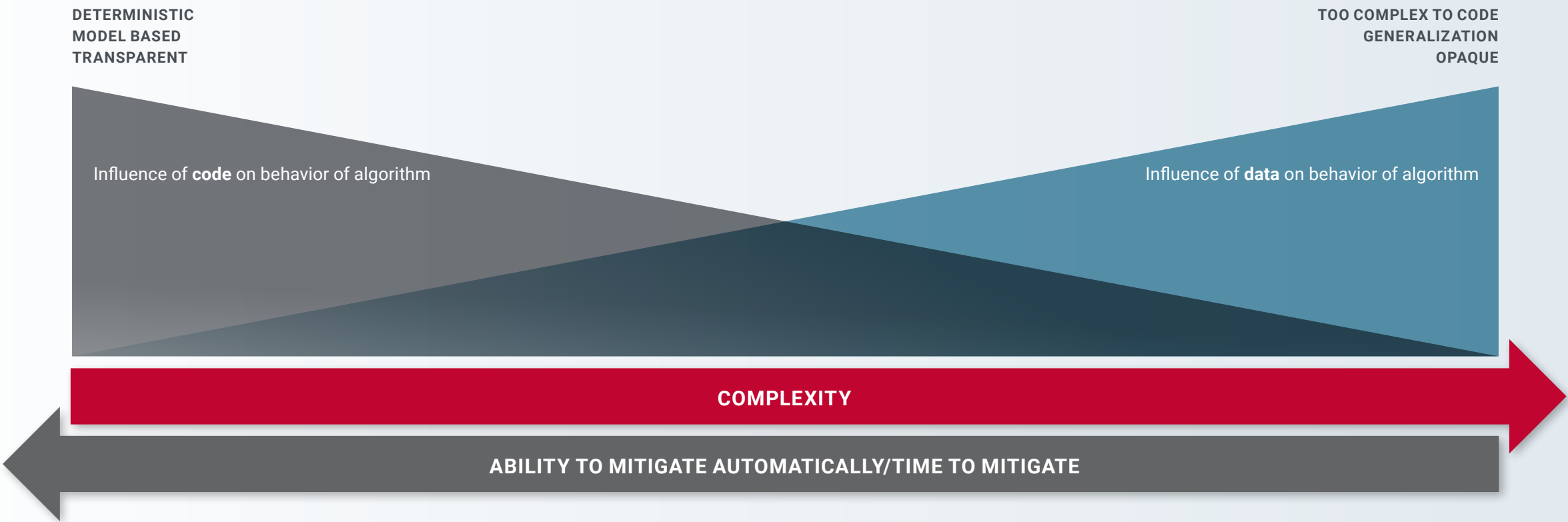
As 5G pushes network functions and data to the cloud, there’s an opportunity to use all that information to better protect against attacks with the help of artificial intelligence (AI) and deep learning.

This is where the “big” in “big data” comes into play. Because 5G virtual devices live on the edge of the network in small appliances, there isn’t enough computing power available to identify evolving attack traffic in the devices. But by feeding traffic through an extra layer of protection at large data centers, it is possible to compile all the data to identify attacks.

A single device or enterprise doesn’t have enough information to characterize an attack. By uploading info to the cloud and combining it with inputs from billions of other devices and thousands of enterprises, AI and deep learning can analyze collective data to predict attacks in the very complex network environments.

MORE DATA, BETTER RESULTS

Detection algorithms and machine learning combine to comb through massive amounts of good data to more accurately identify anomalies in network traffic to alert mobile service providers of threat profiles.





### GAME OF PROBABILITY

AI requires huge amounts of good data to sift through and create neural networks where anomalies can be detected. Good data is key. Bad or poisoned data leads to biased models and false negatives. The more good data, the better the outcomes in this high-stakes game of probability. 5G has the speed and capacity to enable AI with data from 50 billion connected devices.

As all this traffic is fed through the scrubbing centers at data centers around the world, AI can help inform security algorithms to detect protocol anomalies and flag issues. The near real-time process is complicated. Like an FBI watch list, a register of attack info goes to a mobile network's control plane. The result is a threat intelligence feed that uses the power of machine learning to identify and stop attacks.

The best place to populate AI and deep learning systems is from crowd sourcing and global communities where large numbers of enterprises and networks contribute data. Bad data will find its way in, but the good data will significantly outnumber the bad data to make deep learning possible.

### MEET PASCAL GEENENS



- ▶ Cybersecurity and emerging technology thought leader
- ▶ EMEA Security Evangelist for Radware
- ▶ Discovered and reported the BrickerBot attack

*“The landscape of threats from botnets, web scraping and IoT zombies is dynamic and increasingly complex. With 5G on the horizon, it’s critical that mobile service providers make plans now to protect their networks against evolving cybersecurity threats.”*

*As part of the Radware Security Research team, Pascal develops and maintains the IoT honeypots and actively researches IoT malware. Pascal discovered and reported on BrickerBot, did extensive research on Hajime and follows closely new developments of threats in the IoT space and the applications of AI in cybersecurity and hacking.*





# 06

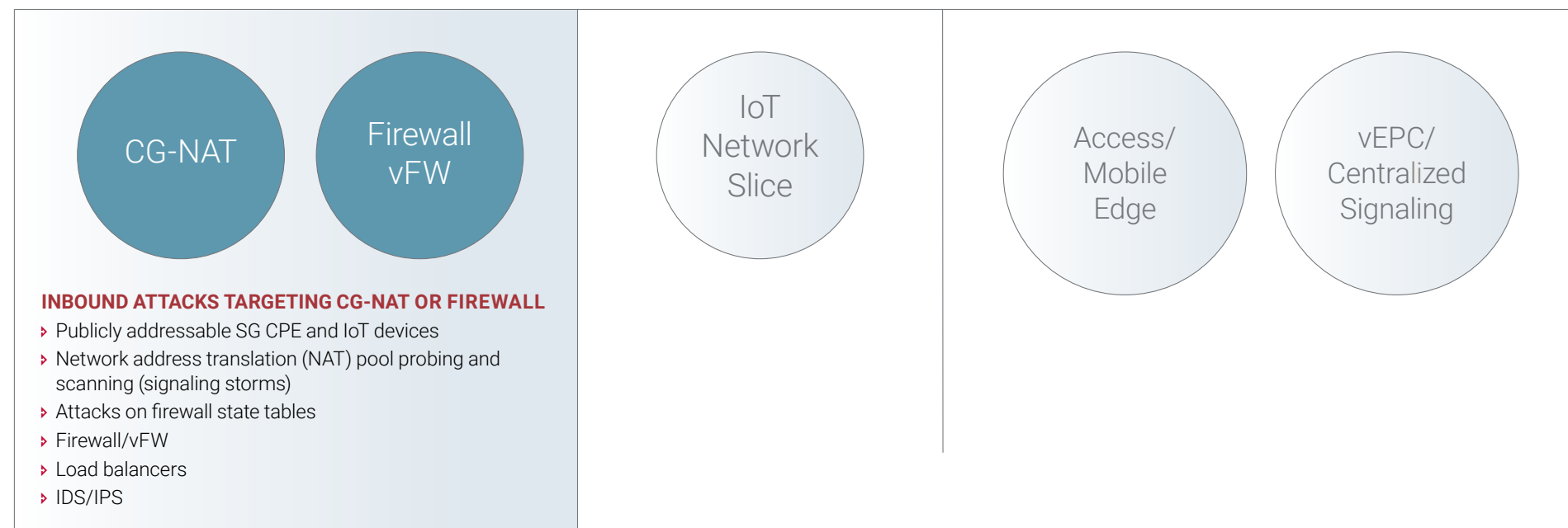
## 5G Security Use Solutions



- Use cases to defend mobile networks include attack protection of stateful devices such as firewalls, and shielding against incoming signaling storms, such as targeting a carrier-grade network address translations (NAT) device.

#### STEP 1: NETWORK AVAILABILITY

*To make sure users have internet access, service providers must protect the stateful devices on the inbound points of their networks. Placing stateless DDoS devices to protect the state tables in firewalls from overflowing, harden firewalls from attack and keep them cost-effective and computationally efficient.*

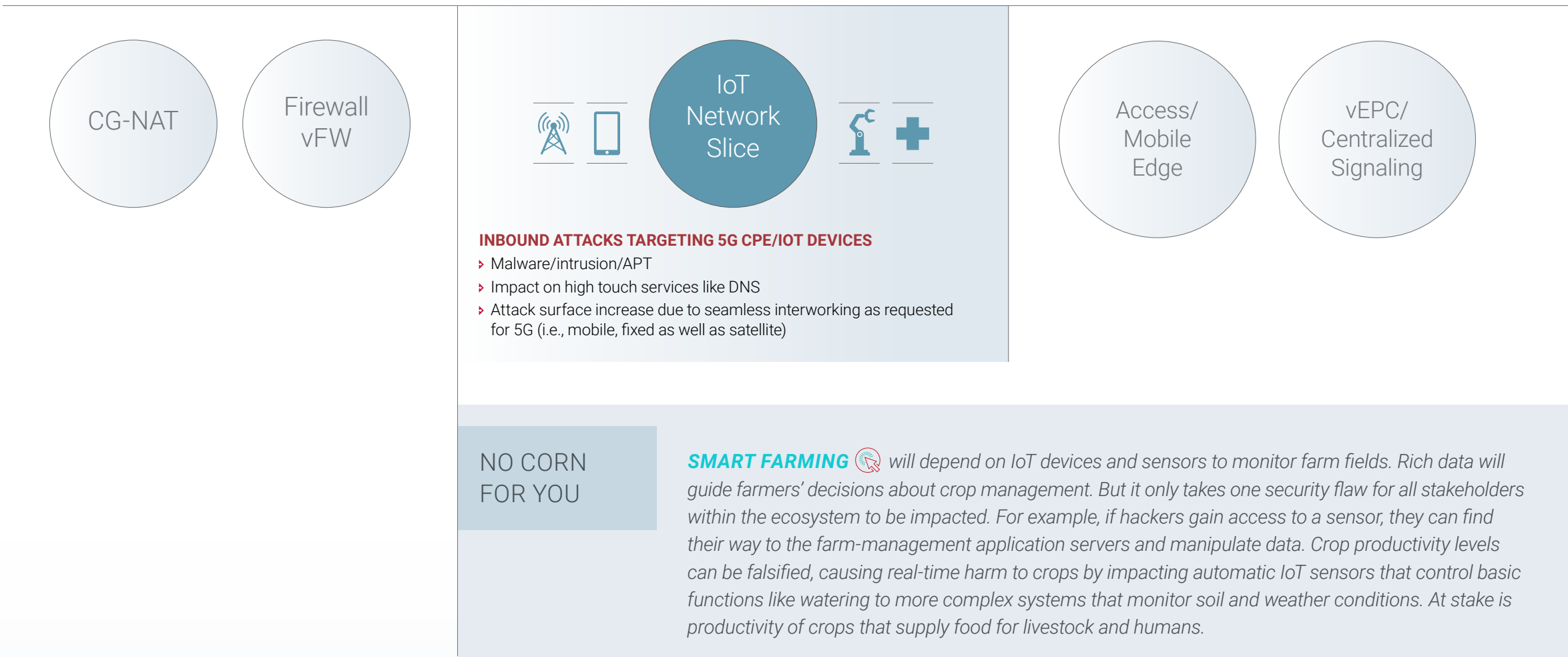


➤ A more advanced use case centered on IoT adoption is the ability to create “secure network slices” as part of the concept of logical partitioning of the network resources in a service-based, software-defined, virtual architecture.

As slices are created for various dedicated service functions in 5G, those same slices can have security built in for protection against malware intrusion targeting 5G and IoT devices as well as specific server attacks like DNS.

STEP 2: IOT DEVICE PROTECTION

To protect the billions of connected IoT devices, good and bad bot traffic must be examined in real time to create a secure IoT ecosystem. By providing an IoT network slice, service providers create an opportunity to monetize this security offering.





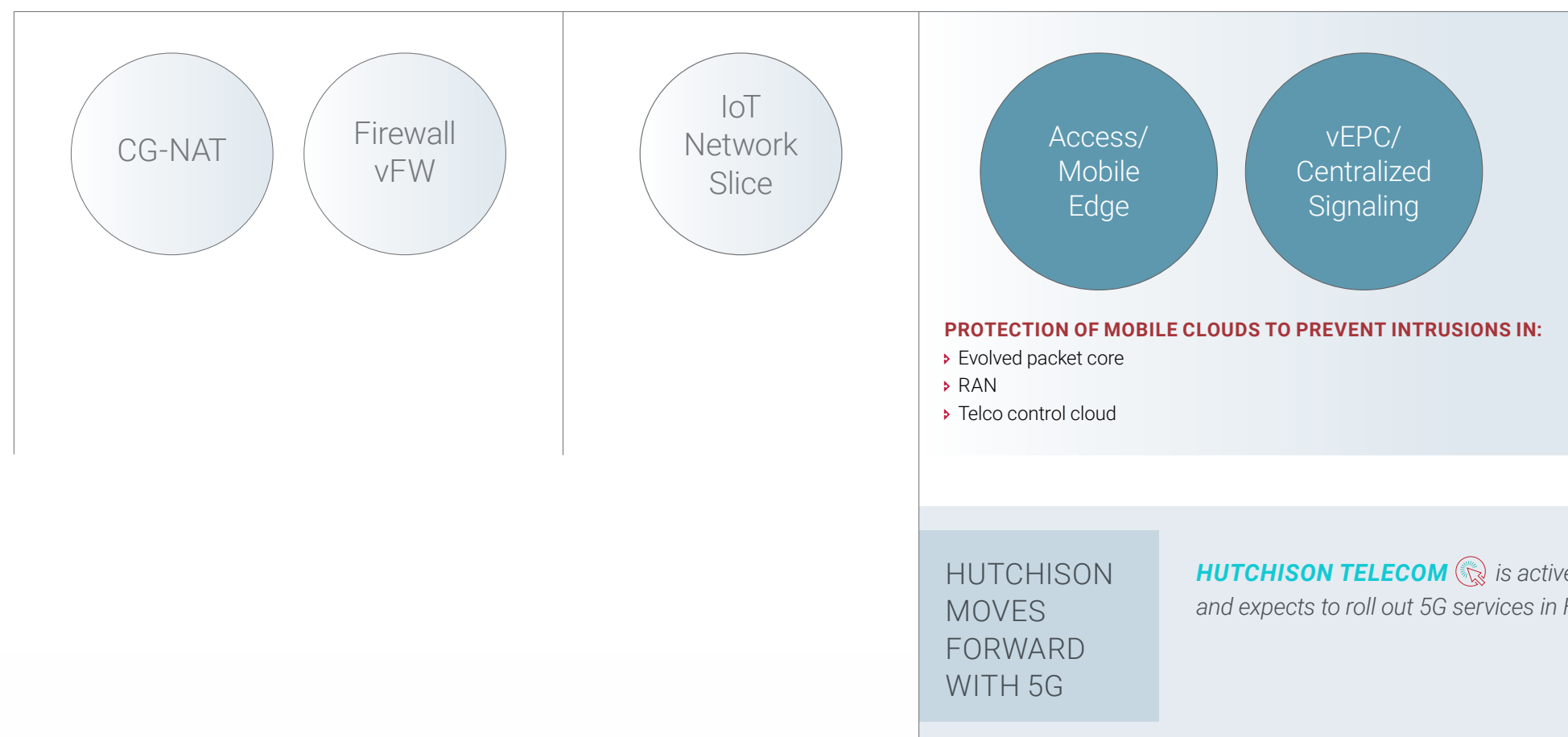
➤➤ 5G is all about “cloudifying” the network — where the RAN and the CORE entities and their interfaces are now all virtual.

As such, there are threats coming inbound and outbound of the virtual instances, so security needs to reside both within and between the clouds. We can envision that there will be clouds composing the RAN and the EPC

specifically, but also a “telco control cloud” for the purpose of orchestration and optimization of all the virtual entities in the network.

### STEP 3: CLOUDIFICATION OF MOBILE ACCESS NETWORKS AND CORE NETWORKS

*In 5G networks, devices are virtual and cloud based. Mobile computing resources are pushed to the edge. Security protections must adapt to protect the new virtual infrastructure. State-sponsored attacks could take down networks across a country.*







# 07

## Summary



## ▶▶ *The Time Is Now*

The deployment of 5G technologies promises to transform how mobile service providers deliver services to consumers and businesses.

Faster speeds. More capacity. And, unfortunately, new and more complex security threats.

The good news is there is still enough time to prepare your security strategy before 5G networks begin to go live in 2020. *Radware can help.*

ALL OF THE 10 TOP-TIER SERVICE PROVIDERS IN THE  
WORLD RELY ON RADWARE'S SECURITY SOLUTIONS TO:

1

Secure their  
network  
infrastructures

2

Create new  
revenue-generating  
services by securing  
IoT devices

3

Support the  
transformation of their  
security tactics as  
they transform to  
cloud-based models

Questions? Tell us a little more,  
or give us a call at **877-524-1419**  
to reach a sales professional.

