BIZCOMMUNITY

# The security implications for 5G and IoT

By Doros Hadjizenonos

28 Jan 2019

The advent of 5G networks is about much more than just incredibly fast speeds and more reliable connections.

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet

When combined with today's powerful edge devices - whether consumer-grade smart devices or the new generation of industrial-grade IoT devices - the impact of 5G on business and networking strategies will be transformational. There are important implications for digital transformation that need to be considered, especially when it comes to securing the new network environments that 5G and edge-based computing will create.

## The impact of 5G

As 5G begins to be widely available, several things will happen:

- In addition to exponentially faster speeds, 5G will also introduce greater capacity, reduced latency and more flexible service delivery.

- Lower latency and highly reliable connections will enable greater edge-based computing without the need for nearby data centres to support latency-sensitive transactions and workflows.

- Eventually, when 5G speeds and capacity are combined with the unprecedented power of edge devices, we will see the creation of new edge-based networks that can share and process information locally, as well as cloud-based resources.

- 5G will also have an impact far beyond interconnecting endpoint devices.

## Examples of 5G and IoT

Enhanced communication services within connected cars, for example, will go well beyond the current set of interactions that already occur internally between onboard IoT devices such as braking, environment monitors, GPS and even entertainment systems.

Live connections between drivers and businesses will enable financial transactions, such as paying for fuel, ordering food at a drive-thru restaurant or paying tolls, without having to pull out a credit card. Communications between vehicles and between cars and infrastructure-based IoT will enable enhanced traffic management and augment things like autonomous driving at highway speeds.

Likewise, there are significant implications for healthcare and medical IoT. 5G speeds will allow the real-time transmission of data to support things like remote surgery, the tracking of monitors and other connected medical devices, including wearable medical IoT, and the analysis of tests and scans by remote professionals.

These advances will not only allow patients to have access to the best physicians in the world, but they will also extend 21st-century medical care to remote locations that currently lack reliable medical resources.

## Security implications for 5G and IoT

These new connected environments will also have serious consequences for security. The biggest challenge will be the sudden, exponential growth of the attack surface due to the rapid expansion of IoT devices and edge-based computing. This will be followed closely by the fact that these devices won’t necessarily be connected to a central network in a traditional hub-and-spoke configuration.

With literally billions of IoT devices interconnected across a meshed edge environment, any device can become the weakest link in the security chain and expose the entire enterprise to risk. Addressing this challenge will require some fundamental shifts in how we think about networking and security.

Security will need to be edge-to-edge, from the IoT edge, across the core enterprise network and out to branch offices and multiple public clouds. Security must also support elastic, edge-to-edge hybrid systems combining proven traditional strategies with new approaches.

Sharing threat intelligence, correlating event data and supporting automated incident response will require security technologies to be deeply integrated.

Interoperability between different security tools will also require establishing new open 5G security standards, the adoption of APIs across vendors and agnostic management tools that can be centrally managed to see security events and orchestrate security policies.
These are just a handful of the security implications resulting from the adoption and deployment of 5G networks.

## Where to start

Many organisations are clearly underestimating the potential impact of the coming 5G revolution and the effect it will have on how they conduct commerce and compete effectively within the next iteration of the digital economy. However, there are a few things that organisations can do now to prepare.

The most effective approach would be to migrate from traditional, isolated point defence products to a security fabric designed to be integrated, automated and open using open APIs and common standards. This approach also need to combine single-pane-of-glass management and control with security technologies that can move seamlessly across traditional, SD-WAN, multi-cloud and highly mobile endpoint and IoT devices for consistent visibility and control.

Organisations that begin preparing now for the security and networking implications of 5G, especially as billions of new IoT devices will be deployed in the next year, will be far ahead of their competitors. And in today’s highly evolving digital marketplace, that difference is likely to be critical.

## ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet

- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...