orange™

VISION 2030: DIGITAL IMMUNITY

A conversation with Hana Kvartová, Chief Commercial B2B Officer at Orange, explores the company's vision for 2030 and how digital transformation is reshaping business infrastructure, cybersecurity, and cloud strategy. As she points out, automation, connectivity, and resilient digital ecosystems will enable enterprises to compete in an AI-driven economy of the future.

HANA KVARTOVÁ
Chief Commercial B2B Officer
Orange Slovakia

As Chief Commercial B2B Officer at Orange Slovakia, Hana is responsible for the company's entire B2B business, including corporate clients and the public sector. She began her career at DIMANO, overseeing B2B sales, call center operations, and marketing.

In 2006, she joined the software and analytics company SAS, where she held senior leadership roles for nearly two decades, managing operations in Slovakia and across six Central European markets, including Poland, Hungary, and the Czech Republic. Over the course of her career, she has built almost 20 years of experience in driving business growth, organizational development, and digital transformation across the region.

How should leaders rethink digital transformation toward 2030?

The year 2030 is not a finish line; it is a state of permanent change driven by automation. Anything that can be automated will be automated. Leaders must understand that digital transformation is no longer a project, it is a core requirement for competitiveness. Customers expect instant answers, and employees demand simple digital tools. At Orange, we are moving away from just selling voice plans or internet lines. Our strategic focus is to build the "digital immunity" and robust infrastructure that can support AI and automation without collapsing. Investments in private networks and edge computing will double by 2030, while cloud and cyber services will grow exponentially. If your network is not intelligent and secure by then, your business will just be an expensive museum piece. What is the real impact of 5G technology beyond mobile speed?

The real strategic breakthrough is 5G Standalone (5G+), a network entirely independent of old 4G infrastructure. For the first time in history, we can guarantee network parameters for specific machines or processes. The game-changing feature here is Network Slicing. Imagine it as reserving your own dedicated lane on a highway where there is never any traffic, even if the whole country is online at the same time. This is crucial for Industry 4.0—whether it is an autonomous warehouse vehicle, a production line, or real-time security cameras. Through our Campus networks, Orange is already deploying 5G SA+ solutions that provide latencies below 10 milliseconds, which Wi-Fi simply cannot handle. If you want to compete globally by 2030, you need to implement this today.

How can expanding companies make their network management more flexible?

The trend is clear: Network-as-a-Service (NaaS) or Managed Networks. By 2030, up to 60% of enterprises will adopt this model. Just as few companies build their own power plants today, fewer businesses want to manage their own hardware. They want a safe service that grows with them. The transition from cables to software happens via our managed SD-WAN solution. It allows you to see your entire network on a single dashboard. If a cable is cut in Nitra, the system automatically switches to a 5G backup within a millisecond.

How can mid-sized companies defend themselves against sophisticated cyberthreats?

You only stand a chance if you do not fight alone. Cyber security is no longer just an IT department issue; it is a boardroom priority. Since attackers use AI and automation, the future of defense lies in ecosystem partnerships and global threat visibility. Currently, the average time to detect a cyber attack is over 200 days—meaning an intruder could be in your network for half a year. To combat this, we invest in our services and integrate closely with Orange Cyberdefense. Our Dynamic SOC (Security Operations Center) platform shortens this detection time to mere minutes. Unlike standard 24/7 SOCs that require massive human teams, this software platform protects your external infrastructure perimeter, endpoints, and online communication environments like Microsoft. It offers mid-sized businesses elite-level protection they could never afford to build internally.

> **Digital transformation is no longer a project, it is a core requirement for competitiveness.**

How should companies approach cloud decisions amid geopolitical uncertainty?

The defining strategic topic today is data sovereignty. European companies are realizing that leaving their critical data "somewhere in a global cloud" carries severe legislative and security risks. Businesses want the benefits of the cloud, but they also want strict control over where their applications run and where their data physically sits. Orange's vision is to provide a safe harbor right here in Slovakia through our certified local data centers. This local cloud approach ensures compliance and safety.

How can businesses manage rising infrastructure costs?

It is true that the AI boom demands immense computing power and more RAM, driving up hardware costs. Our answer to this volatility is Orange S3 Storage. This object storage is the foundation for modern backup. If your business is hit by ransomware, hackers will immediately try to delete your backups. However, on our S3 storage, your data is "locked" and cannot be deleted by anyone—not even you or a hacker—for a predefined period. It is your ultimate insurance policy. Furthermore, we offer flexible Housing services where you can rent entire racks or parts of them. The main benefit is price stability; despite market fluctuations, Orange can guarantee fixed prices for these local, scalable, and highly cost-effective Slovak cloud solutions.