

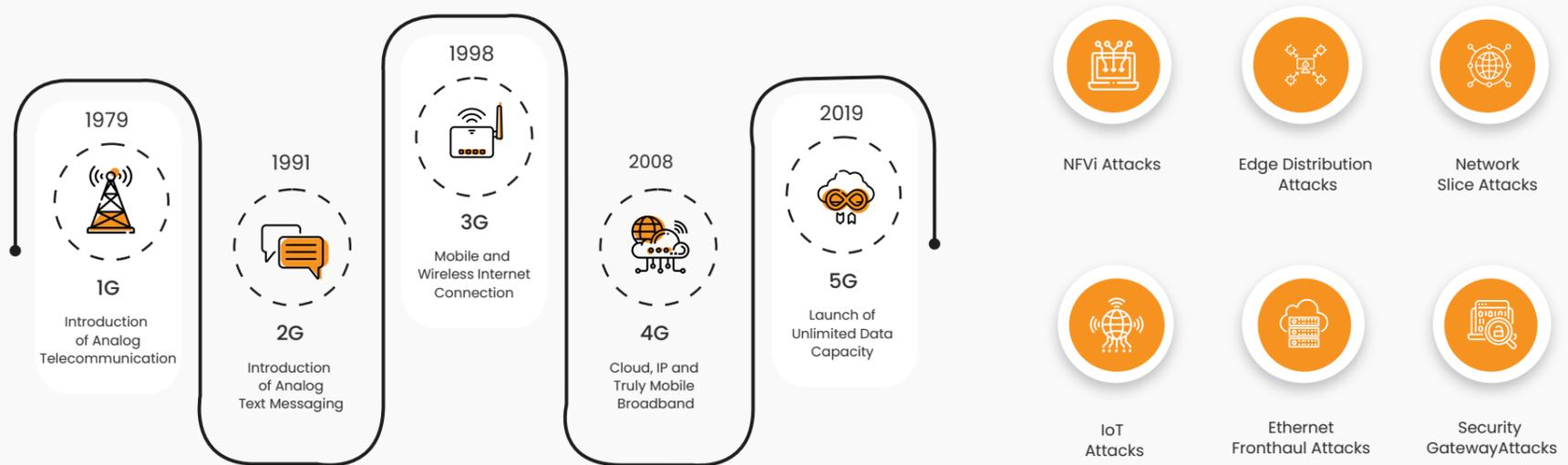
5G NETWORK: THE NEW ERA OF TECHNOLOGY AND RISKS

ENTERPRISE SECURITY APPROACHES DEPEND ON THE BUILD OUT OF 5G AND ENTERPRISE RISK APPETITE

The transition to 5G is unfolding with implementation requiring strategic planning and long-term investment. Organizations should be proactive today, act with purpose, and take action. Many trendsetters have begun their journey to the edge and 5G, setting the pace and cadence for the future of innovation. As additional enterprises join the journey to 5G, those organizations should seek to utilize existing security technologies in building a security road map.

This report highlights the need for a benefit-to-risk evaluation of data security and access management concerns juxtaposed against enhanced speed and reduced latency benefits. This evaluation requires a review of existing security programs, policies, and controls. Other key areas useful for the enterprise to consider as it transitions to 5G are:

- Assess the organization's risk appetite.
- Consider asset and network topology.
- Determine the organization's innovation posture. Evaluate whether the organization is a leader or laggard in a software defined world with the ability to enable a malleable 5G security architecture.
- Identify areas of security in need of immediate attention. Think about which currently deployed security assets can be utilized today that will make the journey to 5G with the business more efficient.
- Align 5G technology and digital transformation strategy with an enterprise-wide strategy. Coalesce a strategic, cross functional tiger team to steer the initiative.
- Envision the end state. Consider segmentation as a first step to Zero Trust or choose an initial focus on creating platform visibility of threat intelligence, analytics, and response tools across existing assets.

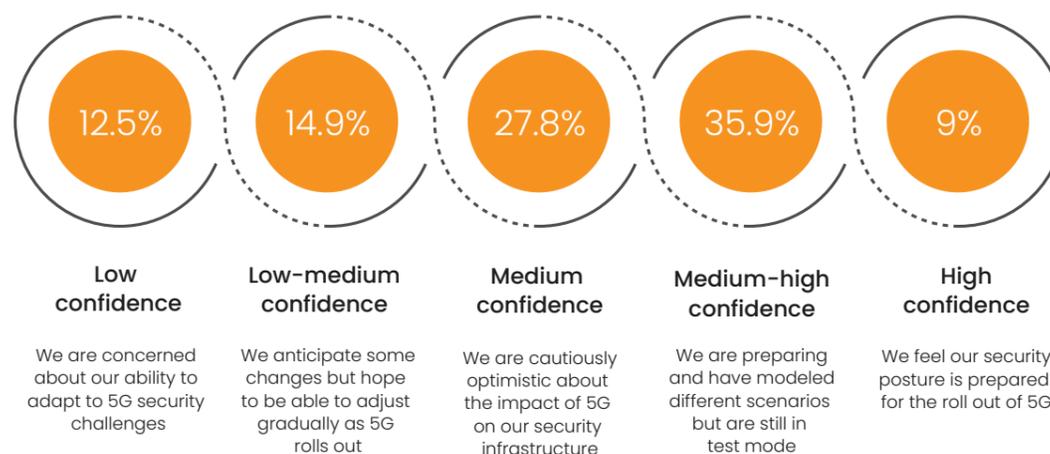


THE EVALUATION OF WIRELESS TECHNOLOGY

5G EXACERBATES SECURITY RISKS

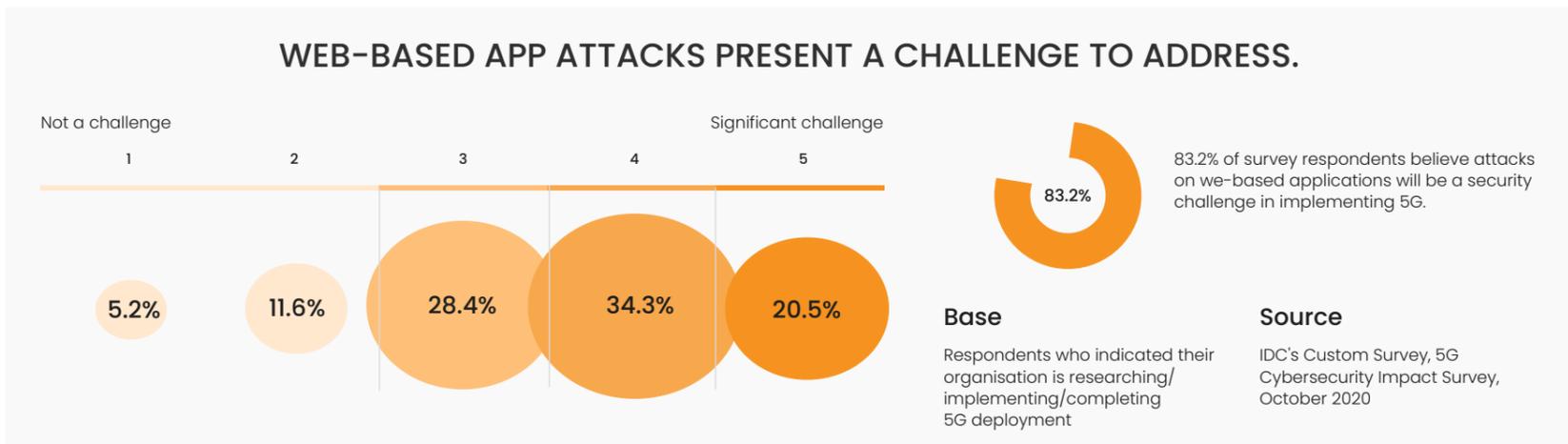
ENTERPRISES ARE CAUTIOUSLY OPTIMISTIC AND PREPARING FOR THE IMPACT OF 5G.

Moving the data processing closer to the use case application certainly allows for near real-time, AI-enabled processing and decision making, but it is not without drawbacks. Along with it comes the possibility of older-style threats such as SQL injection attacks, unencrypted data travelling along private networks that may or may not have malware-sniffing apps looking at the data, and other yet-to-be identified security challenges.



In the near term, 4G will continue to exist. In fact, during the market's transition to 5G, traffic will move between 4G and 5G via roaming exchanges that have been established for 4G. Network operators provide that infrastructure and roaming interfaces at the signaling layer, and they are protected. The enterprise must be responsible for the data layer. A shared security model like that in public cloud is needed.

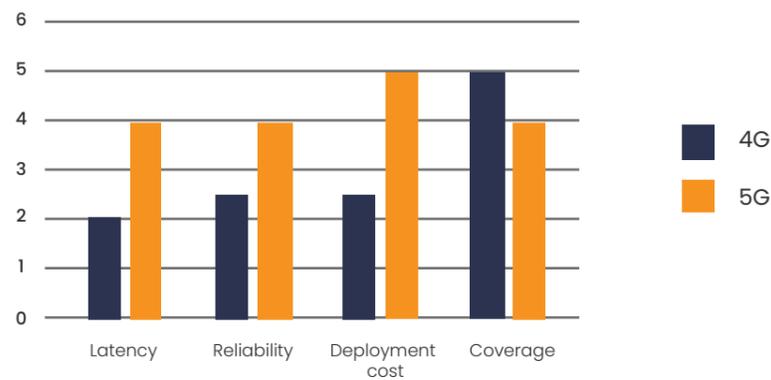
Yes, 5G is revolutionary, and businesses are banking on the capabilities that 5G promises. However, they concurrently recognize the need to team with the right service providers to help user in the capabilities that 5G and edge computing have the potential to deliver in a safe, highly secure, and resilient way.



5G INDUSTRIAL IOT MARKET 2021 SIZE, SHARE, BUSINESS OVERVIEW, FUTURE PROSPECT BY 2027

The remote working across widespread geographies demands a high-speed network, such as 5G, for experiencing higher connectivity and improved performance. Following are the highlights forecasted by research analysts:

- The hardware segment of the 5G industrial IoT includes 5G modules, gateways, sensors, and chips.
- The growth of the managed services segment is expected to be driven by the increased monitoring and security requirements, improved regulatory compliances, enhanced productivity, and improved data integrity while meeting strict Service-Level Agreements (SLAs).
- The market being at the nascent stage, several big firms are launching 5G modules by having partnerships with telecom operators to deploy services at a faster pace.
- 5G combined with IoT-enabled connected worker solution can bring monitoring capabilities to the next level, making workplaces more efficient, transparent, safe, and productive.
- 5G industrial IoT solutions are expected to increase the operational efficiency of the discrete manufacturing process by offering higher connectivity among IoT devices.



4G v/s 5G

ASSURING 5G CYBERSECURITY

The things that make 5G possible is virtualization, migration to the cloud, network slicing, IoT, and even 5G gateways are also potential vulnerabilities. Then there are the added risks from agile software development processes that, in times of a rush to market, raise the risk that code is deployed that has not been adequately tested. The careful observation is critical if the industry is to stay ahead of the changing 5G threat landscape.

SKILLMINE CYBER SECURITY TEAM