5G CYBERSECURITY

To help organizations effectively manage 5G-related security risks, the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) launched the 5G Cybersecurity project. As 5G becomes more widely available, operators and users of these systems must safeguard the technology from cyberattacks as 5G development, deployment, and usage evolves.

NIST is adopting an agile process to publish this content. Each volume is being made available as soon as possible rather than delaying release until all volumes are completed. Work continues on implementing the example solution and developing other parts of the content. As a preliminary draft, we will publish at least one additional draft for public comment before it is finalized.

Throughout this project, if we identify gaps in 5G cybersecurity standards, we will work within the appropriate standards development organizations to address them.

This fact sheet provides an overview of the current state of the 5G Cybersecurity project.

CHALLENGE

5G is at a transition point. Simultaneously, standards bodies are specifying technologies that are being implemented by equipment vendors, deployed by network operators, and adopted by consumers. What's more, current 5G cybersecurity standards mainly focus on the security of standards-based, interoperable interfaces between 5G components. They do not specify cybersecurity protections that organizations can apply to underlying information technology (IT) components that support and operate the 5G system. This information gap makes it harder for organizations to safeguard their 5G network and increases risk from not adequately protecting the IT components that support 5G systems.

PROPOSED SOLUTION

Our proposed solutions build upon the work of the NCCoE's Trusted Cloud project, where hardware-enabled security serves as the foundation of cloud security. We are focused on a combination of 5G standards-based security features as well as a secure cloud-based hosting infrastructure. The result will be a commercial-grade security reference architecture for 5G networks that bridges the gap between IT and telecommunications cybersecurity capabilities.

BENEFITS

By adopting the proposed solutions contained in the *5G Cybersecurity* Practice Guide, organizations can benefit by:

- **Reducing risk and lowering the likelihood of an incident occurring**—from understanding the security capabilities 5G networks can provide.
- **Strengthen their 5G network's supporting infrastructure**—making it more resistant to compromise and having more visibility into the trust status of underlying platforms.
- **Safeguarding the contents of 5G communications and privacy of 5G users**—from eavesdropping and tampering.

LEARN MORE ABOUT NCCOE
Visit https://www.nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

- **Paving the way to zero trust**—by implementing demonstrated practices that mirror key zero trust principles. Under zero trust, once users are properly authenticated and authorized, their access to an organization's network and resources is limited only to the resources they need to perform their jobs.

HIGH-LEVEL ARCHITECTURE

The diagram below depicts the high-level architecture of the NCCoE 5G implementation.

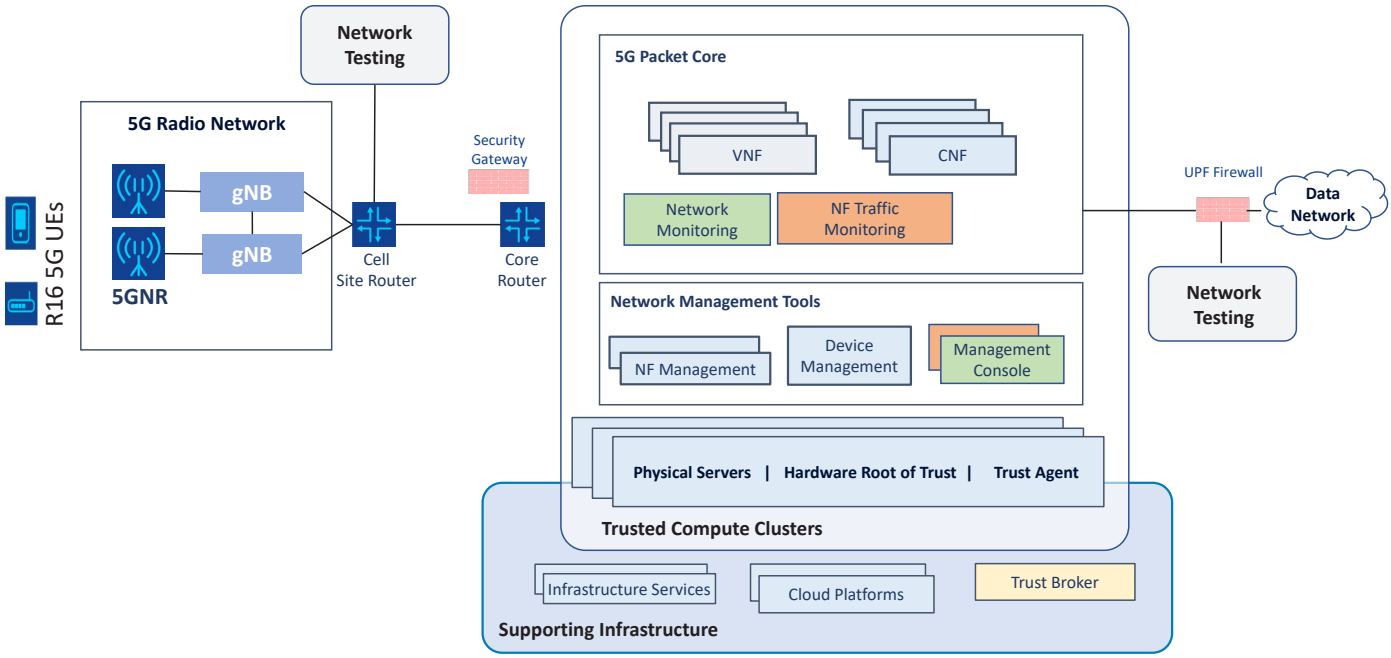
The left side of the diagram represents the 5G radio access network (RAN) consisting of:

- 5G user equipment (UE) (i.e., mobile devices using the 5G network);
- radios and antennas; and
- baseband units (BBUs) known as gNodeBs (gNBs).

The back haul network connects the radio access network (cell sites) and the core network (data center). The data center is a main focus of our example solution and consists of:

- Supporting Cloud Infrastructure enabling Trusted compute clusters
- Network management and security tools
- Virtual and Containerized 5G Network Functions

See Volume B of the *5G Cybersecurity* Practice Guide for more details on the high-level architecture, along with the Data Center Architecture and Trusted Compute Cluster Architecture.



SHARE YOUR FEEDBACK

The comment period to submit feedback for the preliminary draft practice guide **June 27, 2022**. Submit your feedback here or send an email to 5g-security@nist.gov.