Booz | Allen | Hamilton®

# ENABLING 5G SECURITY WITH CONTINUOUS MONITORING

**5G mobile technology will completely transform global telecommunication networks—and mission and business operations.**

# THE 5G SECURITY IMPERATIVE

5G mobile technology will completely transform global telecommunication networks—and mission and business operations. It will forge bonds between physical and digital devices, deliver tremendous performance advantages, help reduce costs, generate massive amounts of data, and enable a connected world on an unprecedented scale. What's more, it will drive federal and defense organizations to expand their ongoing security monitoring activities to the private 5G networks they're developing for a wide range of missions and use cases.

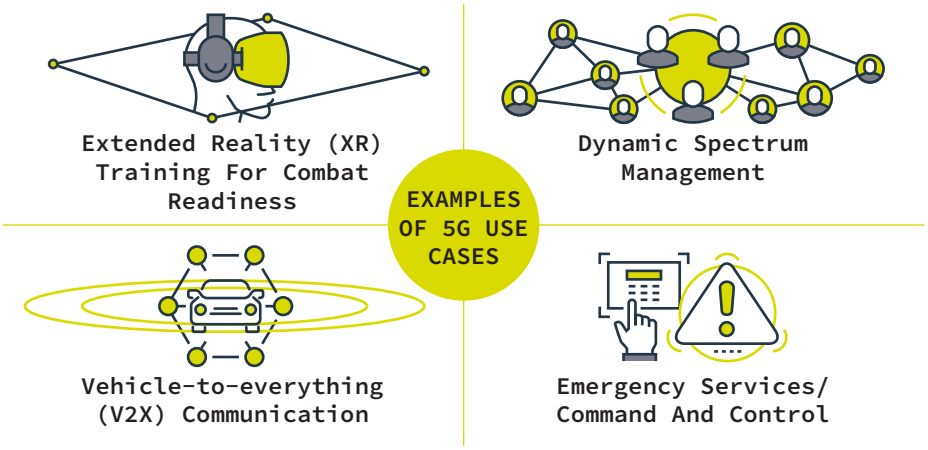
**Here's the problem:** 5G's changes will translate to new vulnerabilities and attack vectors. The deployment of mission-critical Internet of Things (IoT) devices—sensors and controllers, for example—will generate huge volumes of data vulnerable to theft, manipulation, and destruction.

Now, baseline 5G architectures include some security. And organizations are deploying scores of complex cybersecurity tools that emit and absorb data on a massive scale. But many security teams are unable to outpace advanced cyber threats because they can't make the most of their data. Organizations are already drowning in their own data in traditional networks—and the problem will be compounded with the launch of private 5G networks.

**Here's the answer:** Congress has directed the Defense Information Systems Agency (DISA) and U.S. Cyber Command (CYBERCOM) to develop a 5G continuous monitoring capability for non-commercial Department of Defense (DOD) networks. Hence, operators of private 5G networks should implement a continuous monitoring strategy. These organizations need capabilities to provide security monitoring of the network and real-time feedback on the current security posture of the network.

In developing these capabilities, organizations should also embrace data-driven cybersecurity by figuring out how to extract, normalize, and apply increasingly complex and diverse data sets to accelerate security operations—ideally faster than adversaries. To that end, organizations should leverage security analytics, artificial intelligence (AI), machine learning (ML), and automation to collect, manage and use security information to full advantage. These steps can enable security teams to detect anomalies tied to advanced cyber threats.

**OPERATORS OF PRIVATE 5G NETWORKS SHOULD IMPLEMENT A CONTINUOUS MONITORING STRATEGY.**

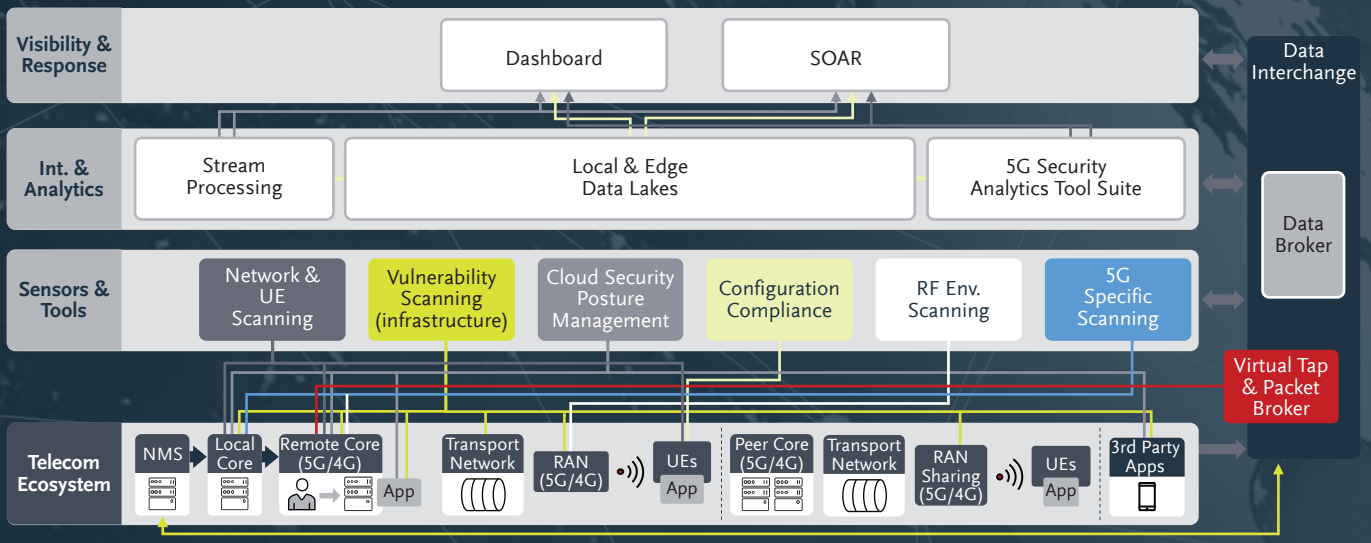


# KEY ELEMENTS OF CONTINUOUS MONITORING FOR 5G SECURITY

End-to-end continuous monitoring for 5G security and resilience involves the entire ecosystem: system users, 5G network functions, the cloud/infrastructure, administrators, operators, vendors, and third-party managed services.

Now, there's lots of relevant U.S. guidance on risk assessments, cybersecurity, and zero trust.[1] But there is no definitive guidance on how to implement data-driven cybersecurity in 5G, so we'll describe leading practices here, starting with a recommended architecture.

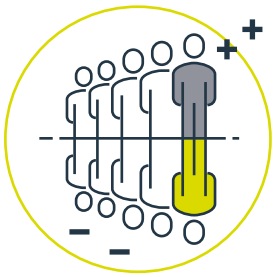
## 5G CONTINUOUS MONITORING ARCHITECTURE




[1] For instance, see National Institute for Standards and Technology (NIST) Special Publications 800-137, 800-53, 1800-33, and 1800-35; the Risk Management Framework (RMF); Cybersecurity and Infrastructure Security Agency (CISA)/National Security Agency (NSA) guidance on 5G cloud security; and CISA and DOD's 5G Security Evaluation Process Investigation Study.

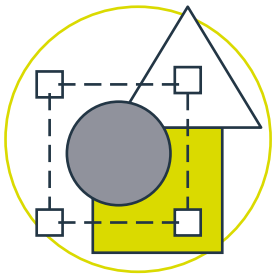
## MAJOR CHALLENGES FOR ANOMALY DETECTION

DESIGNING AND BUILDING SECURITY ANALYTICS | SECURITY



**VOLUME OF DATA**
There aren't enough human analysts to review all the data. Machine assistance and/or a data science solution is needed.

**VELOCITY OF DATA**
New data is generated in the system at a very high rate. The solution must keep up with this rate.



**VARIETY OF DATA**
Every 5G network has different configurations, vendors and features, data formats, and protocols. Solutions must be designed to work despite all this variety.

**ADVANCED THREATS**
Advanced threats to the core network are often overlooked. Many security vendors focus on threats involving user devices, not threats entering the network via other means. Advanced security tools are needed.

This architecture includes the telecommunication system, sensors and tools, the data interchange, integration and analytics, and visibility and response. In addition, it encompasses the various aspects of continuous monitoring, including vulnerability scanning and anomaly detection.

To excel at uncovering anomalies tied to advanced cyber threats, organizations must overcome four major challenges: the volume of data, the velocity of data generation, the variety of data, and cybersecurity gaps involving advanced threats that often aim to infiltrate the core network through means other than user devices.

These challenges are not insurmountable. With a data-driven approach, your organization can analyze massive quantities of cybersecurity data for longer periods in a more cost-effective manner, which unlocks the benefits of security analytics at scale in real time. And this, in turn, can enable advanced cybersecurity that uses predictive analytics and turns threat intelligence into actionable insights.

Here is where the architecture's 5G security analytics tool suite comes in. Your organization can build advanced security analytics for 5G by pairing threat signatures with anomaly detection capabilities designed to spot sophisticated threats. Signatures tied to the discovery of novel vulnerabilities by research teams—like Booz Allen **DarkLabs** with its **carrier-grade 5G Lab**—can provide a reliable basis for spotting advanced adversaries. Network defenders can put such signatures into action by combining them with:

- heuristics for real-time, line-rate anomaly detection
- streaming and big-data ML for near-real-time and/or deep insight
- behavioral network characterization and change detection

Imagine, for instance, a scenario involving rogue 5G user equipment (UE). In this example, the analytics inspecting control and user planes—located in the network and UE scanning portion of the architecture—identify anomalous behavior that shows malicious code has compromised the equipment. This, in turn, triggers an alert to the security orchestration, automation and response (SOAR) platform, which calls the network monitoring system (NMS) to disconnect the UE and prevent it from registering to the network.

This detection capability provides immediate alerts, near-real-time benefits, deep insights over time based on data analysis, and underlying support for cybersecurity visualizations and dashboards. In addition, this approach can elevate security by design with **zero trust**—particularly by building more mature visibility and analytics capabilities that improve detection and reaction time, enabling real-time access decisions. What's more, the network characterization and change detection can help sharpen threat hunting by giving proactive security teams a powerful tool for anticipating and uncovering previously unidentified anomalies. Booz Allen has invented a suite of 5G security analytics tools for all three elements of this approach.

# WHAT'S NEXT:
# STEPS TO TAKE NOW

5G operators need a watchful eye on cybersecurity because determined nation-states won't look away from the chance to target 5G networks and data. To start moving ahead of threats, security teams need to proactively ready data to be analyzed and queried. Operators of private 5G networks can disrupt sophisticated cyber threats by building 5G continuous monitoring capabilities that leverage security analytics, AI/ML, and automation. We recommend that organizations take three steps:

1. Conduct threat modeling and assess risk. Know the priorities of what to protect and how an attacker may go about exploiting those resources. Identify potential weaknesses.

2. Create a scalable adaptive ML workflow and data pipeline. Truly leverage the strengths of both humans (5G, cyber, and data-science experts) and machines in a symbiotic relationship that accelerates and improves the output of both, efficiently processes data, and enables automated defenses, security dashboarding, and proactive threat hunting.

3. Apply security analytics to cover threats in priority order. To address the needs, deploy commercial products as well as custom analytics designed to counter sophisticated attacks by advanced persistent threats.

Organizations seeking help adopting leading practices and demonstrating 5G continuous monitoring capabilities should look for industry partners with uniquely relevant expertise in several areas: 5G security, **zero trust**, and advanced security analytics for countering sophisticated threats; mission-driven insights about the evolving threat landscape and advanced cyber adversaries; key guidance from DISA, NIST, and other agencies; and specialized tools for countering advanced threats.

For more information, contact us at **www.BoozAllen.com/5G**

**WWW.BOOZALLEN.COM/5G**

## EMPOWER PEOPLE TO CHANGE THE WORLD®

For more than 100 years, military, government, and business leaders have turned to Booz Allen Hamilton to solve their most complex problems. As a consulting firm with experts in analytics, digital solutions, engineering, and cyber, we help organizations transform. We are a key partner on some of the most innovative programs for governments worldwide and trusted by their most sensitive agencies. We work shoulder to shoulder with clients, using a mission-first approach to choose the right strategy and technology to help them realize their vision.

With global headquarters in McLean, Virginia, our firm employs approximately 29,500 people globally as of March 31, 2022, and had revenue of $8.4 billion for the 12 months ended March 31, 2022. To learn more, visit www.boozallen.com. (NYSE: BAH)