Booz | Allen | Hamilton®

BUILDING MISSION-DRIVEN 5G SECURITY WITH ZERO TRUST

EMBRACE A LEADING MINDSET FOR BETTER PROTECTION

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

Putting zero trust into action today with existing tools can mitigate emerging mission risks and enable the 5G capabilities of tomorrow.

BUILDING MISSION-DRIVEN 5G SECURITY WITH ZERO TRUST

Now more than ever, national security missions must overcome risks around untrusted technology in a hyperconnected world. To enable resilient operations and shield sensitive data through these challenges, the Department of Defense is urging its senior leaders, engineers, operators, and contractors to embrace a "zero trust" security model for sensitive data, systems, and services, including fifth-generation (5G) mobile technology. All networks should leverage this mindset. And putting zero trust into action today with existing tools can mitigate emerging mission risks and enable the 5G capabilities of tomorrow. Here's what you need to know to get started.

IT'S ZERO HOUR FOR ZERO TRUST

The concept of zero trust has been around for years— but it's never been more vital for national defense. This shows in Executive Order 14028 and in the National Security Agency's guidance on embracing zero trust for critical networks like national security systems, DoD networks, and defense industrial base systems.[1] And DoD's 5G Strategy Implementation Plan declared zero trust is "ideally suited for the emerging 5G network infrastructure."[2] There is no turning back. Now is the time to explore, commit to, and embark on this path. Leading organizations that proactively adopt this approach will be better positioned for mission success.

For too long, cyber threats have accelerated while IT security lagged behind. Doubling down on perimeter defenses isn't sufficient now and won't be in the future. Embracing zero trust now is about stepping up and owning the risk that threats can emerge inside, not just outside, traditional network boundaries—and it's also about proactively countering these risks by design.

The zero trust model relentlessly questions the premise that users, devices, and network components deserve to be trusted just because they're in the network. Applying this mindset can help protect critical data in real time from dynamic threats. This involves deploying comprehensive security monitoring, granular dynamic and risk-based access controls, and system security automation in a coordinated way throughout infrastructure. All of this is driven by core principles: assume a breach; never trust, always verify; and allow only least-privileged access based on contextual factors.

To be sure, embracing zero trust in 5G is uniquely challenging—that's because 5G will usher in so much change. Fifth-generation technology will completely transform global telecommunication networks. Billions more devices, sensors, and systems will be connected worldwide. Downloads will be much faster, latency will be much lower, and the capacity to connect more devices to the network will skyrocket. But proactively committing to zero trust could help organizations get ahead of challenges that might rapidly mount as 5G rolls out.

The tremendous performance advantages of 5G are already creating new opportunities for national defense capabilities. DoD is exploring how to use 5G for autonomous vehicles; intelligence, surveillance and reconnaissance; command and control; logistics and maintenance; and training systems featuring augmented and virtual reality. And, according to DoD's 5G Strategy Implementation Plan, the department expects to implement transformational innovations such as "wireless, ubiquitous connectivity" across humans, machines, and the internet of things (IoT).[3]

But 5G also brings new risks. The technology could increase the attack surface for malicious actors by introducing new vulnerabilities and expanding the number of potential targets. And to "operate through" existing 5G infrastructure worldwide, DoD will need to overcome "significant security vulnerabilities" that adversaries could exploit on a global scale, the department's plan says. In some cases, operating through 5G will mean relying on public and untrusted telecommunications infrastructure in the United States or coalition partner countries. More risky operations might depend on "gray zone" network infrastructure shaped or controlled by organizations that don't share DoD mission goals.[4] Operations in contested areas would face the toughest security risks.

And even when DoD has the OK to operate on a 5G network, the underlying equipment could have the capability to detect and disrupt DoD communications. In addition, the department faces the broader risk that adversaries could aim to sabotage missions and equipment, compromise operational security and jeopardize the lives of military leaders and warfighters.[5]

To be sure, 5G networks will bring some network security enhancements. But, as the Government Accountability Office noted in a recent study, many of those won't come until the deployment of complete "standalone" networks. In addition, 5G network hardware will still face supply chain risks. And so, 5G's emergence should drive organizations to adopt zero trust as soon as possible.[6]

Organizations with national security missions must implement zero trust architecture not only in 5G networks they directly control but also over 5G networks owned and operated by others.

BUILD STRONGER SECURITY WITH 7 PILLARS

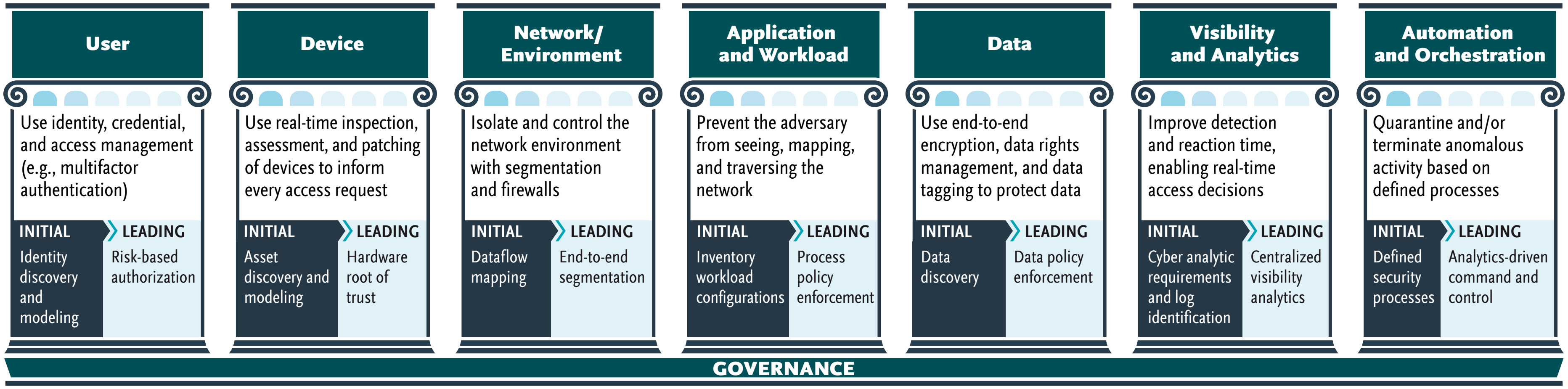
Adopting zero trust requires a culture shift—and that's hard. In addition to owning the "assume breach" mentality, organizations need to integrate the security model into their data-protection strategy, break down organizational and programmatic silos, and gain and maintain buy-in from senior leadership and other key stakeholders. As the NSA notes, integrating zero trust principles within large enterprises can be complicated. Organizations may not fully support zero trust efforts. In addition, zero trust needs to be scalable, which requires a robust infrastructure. And keeping up a persistent mindset is difficult.

In addition, a congressional watchdog has noted developing 5G cybersecurity standards and best practices will be hard; controls will have to be continually updated; and adopting 5G cybersecurity measures will require resources that may exceed what some organizations can do.[7]

Booz Allen recommends using 7 pillars of zero trust, plus governance, to understand the strengths and gaps in current capabilities, and to design actionable plans for improved security.

ELEVATE SECURITY BY DESIGN WITH 7 PILLARS OF ZERO TRUST

Maturity model enables focused improvement, in several steps, from initial practices toward leading capabilities



Pillar		INITIAL	LEADING
User	Use identity, credential, and access management (e.g., multifactor authentication)	Identity discovery and modeling	Risk-based authorization
Device	Use real-time inspection, assessment, and patching of devices to inform every access request	Asset discovery and modeling	Hardware root of trust
Network/ Environment	Isolate and control the network environment with segmentation and firewalls	Dataflow mapping	End-to-end segmentation
Application and Workload	Prevent the adversary from seeing, mapping, and traversing the network	Inventory workload configurations	Process policy enforcement
Data	Use end-to-end encryption, data rights management, and data tagging to protect data	Data discovery	Data policy enforcement
Visibility and Analytics	Improve detection and reaction time, enabling real-time access decisions	Cyber analytic requirements and log identification	Centralized visibility analytics
Automation and Orchestration	Quarantine and/or terminate anomalous activity based on defined processes	Defined security processes	Analytics-driven command and control

GOVERNANCE

GETTING STARTED

Booz Allen recommends employing four complementary steps to realize zero trust for 5G.

1. **Diagnose:** It starts with taking stock of your current capabilities, evaluating their maturity and effectiveness relative to the threats you face, and identifying critical gaps.
2. **Design:** Armed with a threat-centric understanding of where you are, set a target for where you need to be to reduce risk and use that target to align your zero trust strategy and roadmap.
3. **Develop:** Support strategies with a zero trust architecture and technical designs and use vendor assessments to identify the right solutions for your needs.
4. **Deploy:** Operationalize your design by configuring and integrating solutions that close critical gaps across the pillars of zero trust.

Operators of 5G ecosystems need holistic security that includes zero trust architecture, 5G development, security and operations (DevSecOps), and a 5G workforce, as well as vulnerability research and embedded security. Zero trust principles can spread through the entire 5G architecture when analytics and automation are used to drive security improvements over time with policy updates aligned to the other pillars. The continuous development and deployment of new policies protects application authentication and access into the 5G network.

Standing up a 5G security operations center (SOC) puts policies into action with proactive threat hunting, vulnerability management, and event monitoring. This approach helps protect all levels of the 5G network from unauthorized access with continuous monitoring based on policies pushed from the mobile core.

In addition, zero trust principles can enable operations though untrusted networks. We recommend building confidence at the device level, establishing a tamper-resistant hardware root-of-trust, ensuring the identity and boot integrity of forward-deployed devices through remote attestation, and bootstrapping encrypted protocols with identity certificates stored in hardware. Automating the provisioning and lifecycle management of keys and certificates on edge devices will build confidence in edge deployed solutions to support future missions worldwide.

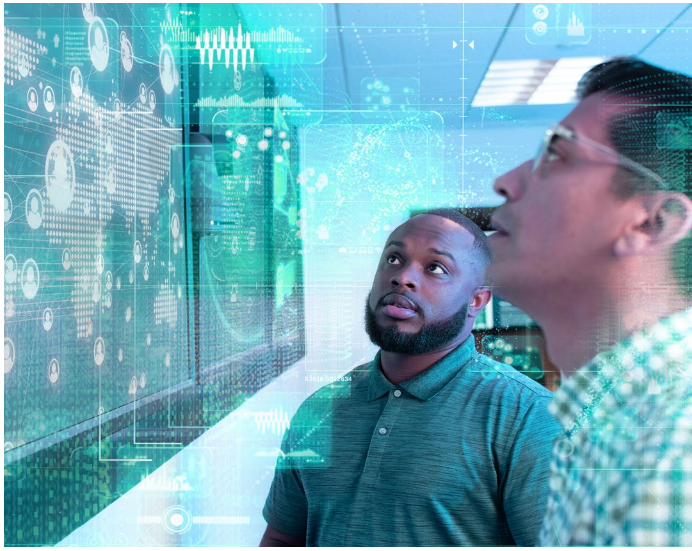
SOFTWARE SUPPLY CHAIN SECURITY

Software supply chain security is critical for 5G because 5G is software centric. To build and/or operate a network, and even to establish connectivity over untrusted 5G networks, operators and organizations will rely on three types of software: third-party software from network and security vendors to manage, operate, and monitor the network; open-source software; and/or software developed by internal teams to automate configurations and operations of the network.

We recommend a DevSecOps methodology that enables continuous deployment of new infrastructure and apps by implementing software supply chain security principles. These principles should guide efforts to build and operate 5G capabilities:

- Use zero trust policies aligned to the pillars to enforce compliance before granting applications access to the 5G ecosystem.
- Drive the continuous delivery of secure applications and infrastructure as code in a software-centric environment while honoring the nuances and distinct requirements involved.
- Use automated security to quickly spot risks in a fast-moving, dynamic 5G environment.
- Complete successive checks for security, risk and compliance to inspect dependencies, open-source code, templates, container images, and running applications.
- Ensure third-party systems comply with your organization's rigorous security standards.

Of course, zero trust isn't a checklist, but rather a mindset that needs to be understood and supported at all levels of an organization to be successful. When embarking on this path, organizations should focus not only on designing zero trust architecture, but also on building, operating and sustaining the approach, as well as supporting it with vulnerability research and embedded security. And increasingly, it will be important to leverage prototyping and research to address emerging 5G use cases—that's why Booz Allen has invested in its new carrier-grade 5G Lab, as well as DarkLabs, an elite team of security researchers, penetration testers, reverse engineers, network analysts, and data scientists, dedicated to stopping cyber attacks before they occur and bringing vulnerabilities to light.



ENVISION—THEN ACHIEVE—ZERO TRUST'S POTENTIAL

NSA plans to issue further guidance on zero trust. But your organization can begin embracing this security model for 5G now. And zero trust isn't a vendor buy: Your organization can do a lot with what it has today.

To illustrate the potential of zero trust in 5G, here are two hypothetical scenarios using tactics and techniques from the MITRE ATT&CK® knowledge base. In our first 5G example, we show how zero trust could mitigate the risk that 5G threat vectors might be used to steal or sabotage sensitive defense technology.

Protecting sensitive technology

	1 NETWORK EFFECTS	2 INITIAL ACCESS	3 CREDENTIAL ACCESS	4 PERSISTENCE	5 PRIVILEGE ESCALATION	6 LATERAL MOVEMENT	7 COLLECTION	8 IMPACT
HYPOTHETICAL 5G THREAT SCENARIO	To spy on a key federal office, a sophisticated threat actor gains access to a nearby 5G small cell and configures the small cell to enable 4G spoofing, which allows the attacker to downgrade the attached devices to a more vulnerable 4G technology and exploit legacy SS7/Diameter vulnerabilities.	Using intelligence gains from espionage, the malicious actor secretly modifies legitimate 5G software used by government and industry, resulting in a software supply chain compromise. This advances a scheme to undermine U.S. defense capabilities.	To further undermine a misconfigured standalone 5G network, the threat actor exploits a packet flow control protocol (PFCP) vulnerability to redirect / intercept communications—with the added power to delete session data or deny service at will. The enemy steals credentials.	Aiming to exploit vulnerabilities in order to craft attack vectors through the attack surface to reach assets, the attacker compromises credentials, gaining access a virtual machine (VM) on the core cloud, part of a customized virtual network function (VNF).	The adversary, an expert at crafting attack vectors on 5G architecture, conducts a hypervisor/ container breakout to gain access to the underlying virtual resources, and subsequently the other underlying infrastructure used by a defense contractor.	The adversary pivots to the underlying host infrastructure used by a defense contractor to steal and manipulate sensitive data.	The adversary is postured to scrape sensitive data,pivot to other infrastructure components, or disrupt/degrade the environment.	The adversary steals—and manipulates—the designs of a new weapons system in development. The sabotaged system fails operational testing and can't be fielded to warfighters. Reputations suffer. Taxpayers must foot the bill.
MITRE ATT&CK® TECHNIQUES	Downgrade to Insecure Protocols	Supply Chain Compromise	Network Traffic Capture or Redirection	Valid Accounts	Escape to Host	Use Alternate Authentication Material	Data from Cloud Storage Object	Transfer Data to Cloud Account & Data Manipulation
HOW ZERO TRUST CAN HELP	Encrypt network traffic. Use security awareness training and zero trust culture. Use firewalls, intrusion detection/ prevention systems and interconnection filtering to counter legacy SS7/Diameter exploitation. *Key pillars: Network/ Environment*	Drive adoption of software supply chain security principles across the whole ecosystem, with implementation tailored to fit each individual stakeholder organization. *Key pillars: Devices, Application and Workload*	Author specific zero trust policies for the mobile core. Use vulnerability log and alert data to spot threats fast—and to improve policies and embedded security for 5G. *Key pillars: Network/ Environment, Visibility and Analytics*	Enforce more layers of inspection, validation, and access controls to prevent abuse of legitimate network access. Integrate multifactor authentication. *Key pillars: User, Network/ Environment*	Use endpoint detection and response on VMs. Configure VMs and containers to deny attackers the ability to access more virtual resources. Use security products at abstracted layers of the cloud core. *Key pillars: Device, Visibility and Analytics, Automation and Orchestration*	Limit permissions to the least privilege needed. Limit credential overlap. Use automation and human experts, including retrained 5G SOC engineers, to proactively hunt and detect threats. *Key pillars: User, Visibility and Analytics*	Implement robust identity and access management. Ensure greater network segmentation for sensitive data to protect it in the event the mobile core is breached by nation-state adversaries. *Key pillars: User, Network/ Environment, Data*	Overall, more stringent authentication measures, network segmentation, and evolved threat hunting can counter advanced threats.

In our second 5G example, we show how zero trust could mitigate risks associated with “operating through” a 5G network abroad.

‘Operating through’ a 5G network

	1 RECONNAISSANCE	2 NETWORK EFFECTS	3 INITIAL ACCESS	4 PRIVILEGE ESCALATION	5 LATERAL MOVEMENT	6 REMOTE SERVICE EFFECTS	7 NETWORK EFFECTS	8 IMPACT
HYPOTHETICAL 5G THREAT SCENARIO	A foreign intelligence service plots to endanger a U.S. person who is performing a critical mission abroad. The enemy’s espionage and sabotage scheme will exploit vulnerabilities in a 5G mobile device and 5G-capable connected car.	A well-positioned 5G network under the adversary’s control connects with the U.S. target’s roaming 5G mobile device, enabling eavesdropping on confidential communications.	Through its shifty 5G network, the enemy sends the device a malicious message to exploit a software vulnerability. This enables access to the device and credentials, as well as the capability to wipe the device at will. The target is none the wiser.	The adversary uses malware to expand access to a mobile device application that supports the 5G functionality of the connected car. The attacker is now poised to take control of the car.	The adversary uses its 5G network and its access to the connected-car application on the mobile device to remotely take control of the car’s steering and braking systems, setting a crash in motion.	The enemy first steals all data on the mobile device and then remotely wipes it to destroy forensic evidence. The aim of the data-integrity attack is to complicate any future incident investigation and enable deniability.	As a failsafe to maximize the crash risk, disrupt 5G-enabled navigation, and delay any rescue, the enemy has on standby an unmanned aerial system with a jammer capable of disrupting another nearby 5G network.	The foreign intelligence service advances its objectives by endangering the target, disrupting U.S. operations, stealing sensitive data, covering its tracks, maintaining deniability, and honing offensive cyber capabilities.
MITRE ATT&CK® TECHNIQUES	**Gather Victim Identity Information**	**Eavesdrop on Insecure Network Communication**	**Exploit via Radio Interfaces**	**Code Injection**	**Exploitation of Remote Services**	**Remotely Wipe Data Without Authorization**	**Jamming or Denial of Service**	**Delete Device Data and Damage to Property**
HOW ZERO TRUST CAN HELP	Limit availability of sensitive data to external parties. Proactively implement robust identity and access management and secure updates for connected devices. Boost vigilance with security training and zero trust culture. *Key pillars: User, Device, Data*	Assume a breach. Enforce use of mutually authenticated encrypted communications from endpoints. Obfuscate communications. *Key pillars: User, Data*	Use endpoint security to classify files as malicious or benign, run unknown files in a sandbox, analyze sandbox-resistant files, block device scans, and block vulnerability analysis and exploitation. *Key pillars: Device, Visibility and Analytics, Automation and Orchestration*	Use endpoint security to detect privilege escalation of user or process, pause or suspension of processes, malware installation from uncommon locations or peripheral devices, and changes in application file size or hash value. Use multifactor authentication. *Key pillars: User, Device, Visibility and Analytics*	Use endpoint security to contain the execution of applications and processes, quarantine file samples, log detailed security event data, and restrict execution of files outside of a known environment and from peripheral devices. *Key pillars: Device, Automation and Orchestration*	Use endpoint security to limit access to enterprise data and resources when connected to unmanaged networks. Protect account credentials. Use multifactor authentication. *Key pillars: User, Device, Data*	Explore emerging ways to counter jamming like beamforming, synchronization signal blocks, and dynamic spectrum sharing technology. *Key pillar: Device*	Applying zero trust at the endpoint can help prevent, detect, and respond to advanced threats when users travel outside the enterprise perimeter and connect to unmanaged networks.

With a zero trust mindset, the national security community can protect highly connected devices and methods of network access and prepare today for the speed and power of tomorrow's 5G-enabled capabilities. Now is the time to take stock of your challenges and risks and set a path toward zero trust for 5G. The success of future missions hangs in the balance.

ENDNOTES:

[1] U.S. President, Executive Order, "Executive Order 14028 of May 12, 2021," Federal Register Vol. 86, no. 93 (May 17, 2021), https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity; U.S. National Security Agency, Embracing a Zero Trust Security Model (Maryland, 2021), https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.pdf

[2] U.S. Department of Defense, Department of Defense 5G-Strategy Implementation Plan (Washington, DC, 2020), https://www.cto.mil/wp-content/uploads/2020/12/DOD-5G-Strategy-Implementation-Plan.pdf

[3] Ibid.

[4] Ibid.

[5] U.S. Government Accountability Office, Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD, GAO-17-668, (Washington, DC, 2017), https://www.gao.gov/products/gao-17-668

[6] U.S. Government Accountability Office, 5G Wireless: Capabilities and Challenges for an Evolving Network, GAO-21-26SP, (Washington, DC, 2020), https://www.gao.gov/products/gao-21-26sp

[7] Ibid.

About Booz Allen

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, 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 its 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 nearly 27,700 people globally, and had revenue of $7.9 billion for the 12 months ended March 31, 2021. To learn more, visit **BoozAllen.com/5G**. (NYSE: BAH)