Booz Allen®

Hardening 5G Infrastructure

Tools and Strategies to Defend Against Salt Typhoon

Developed in partnership with:

paloalto® NETWORKS

Approved for Public Release. February 2026.

Executive Summary

The security of 5G infrastructure is a national imperative and is under direct threat from sophisticated nation-state actors like Salt Typhoon, an Advanced Persistent Threat group. This white paper, a joint effort by Booz Allen and Palo Alto Networks, outlines critical strategies to defend against the tactics, techniques, and procedures (TTPs) observed in recent devastating attacks on telecommunications.

Salt Typhoon executes a full-attack kill chain, leveraging stolen credentials, supply chain exploits, and living-off-the-land techniques to achieve long-term, stealthy access—sometimes lasting years—to exfiltrate highly sensitive data, including subscriber details and network configuration files.

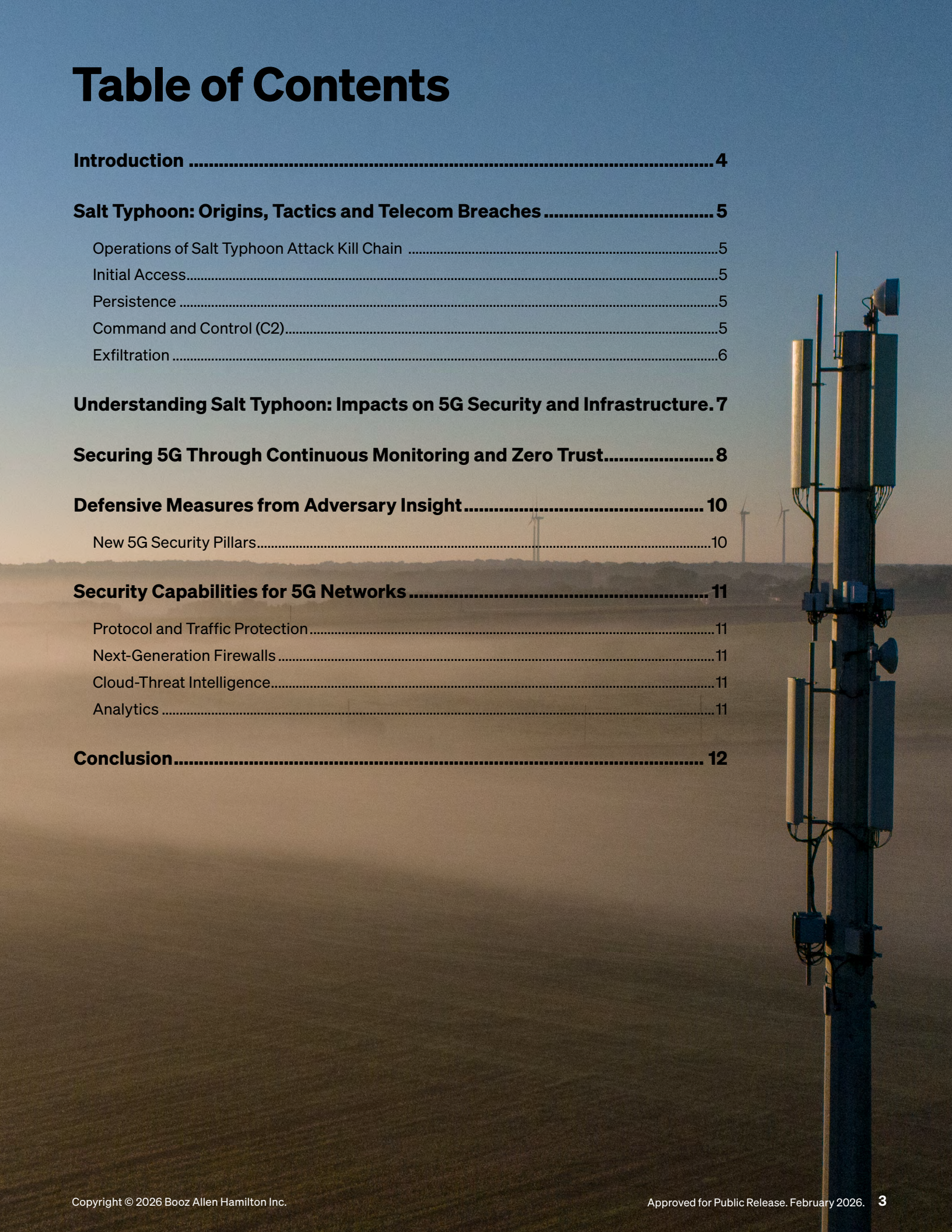
To combat this, organizations must adopt a secure-by-design approach centered on Zero Trust Architecture (ZTA) and continuous monitoring across the entire 5G ecosystem.

Key defensive measures include:

- **AI/Machine Learning-Driven Continuous Monitoring:** Implementing advanced analytics to manage massive data volume and detect subtle malicious behavior
- **Proactive Security Operations:** Regularly conducting security assessments, 5G red teaming, and threat hunting to validate controls and adapt to evolving adversary TTPs
- **Layered Security Capabilities:** Utilizing next-generation firewalls, protocol protection, and cloud-threat intelligence that incorporate behavioral analytics to identify and stop evasive attacks, aligning defenses with adversary models like MITRE ATT&CK and MITRE FiGHT, both owned by the MITRE Corporation

By adopting these proactive and layered measures, operators and government agencies can significantly enhance cyber resilience and protect mission-critical 5G deployments.

Table of Contents



Introduction

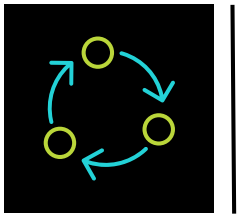
As 5G networks become an asset for national security, defense operations and critical infrastructure protecting them from cyber threats are strategic necessities. The rise of sophisticated threat actors, such as Salt Typhoon, highlights the importance and the sense of urgency for security in 5G architectures. From the core to the edge, the attack surface has expanded dramatically, impacting not only public mobile networks but also private deployments supporting military communications, smart infrastructure, and mission-critical applications.

Booz Allen and Palo Alto Networks combine deep expertise in national defense and cybersecurity to provide insight into how adversaries like Salt Typhoon target the 5G ecosystem. This report explores the origins of Salt Typhoon, and their attack kill chain and provides cybersecurity approaches and solutions to show how large mobile network operators, government agencies, and private operators can proactively secure, reduce, and eliminate risks and improve public and private 5G infrastructure.

Salt Typhoon: Origins, Tactics and Telecom Breaches

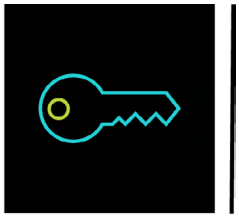
Salt Typhoon is an attributed nation-sponsored Advanced Persistent Threat (APT) group linked to the People's Republic of China. According to United States government officials, this group emerged in early 2022 and is believed to be responsible for targeting telecommunications, control systems, and critical infrastructure. Their alleged focus is to seek long-term access to sensitive communications, enabling espionage and surveillance. Initial reports linked Salt Typhoon compromises to some U.S. telecommunication providers and explained how they leverage living-off-the-land techniques, supply chain exploitation, and custom malware to evade detection. These attacks compromised a wide variety of telecommunication devices, providing them with access to highly sensitive data. U.S. Senator Mark R. Warner called the attack "the worst telecom hack in our nation's history—by far" in the Washington Post.

In August 2025, a Joint Cybersecurity Advisory detailed the tactics, techniques, and procedures (TTPs) the APT group uses and emphasized their primary focus on remaining undetected and maintaining access to systems that will facilitate data exfiltration.



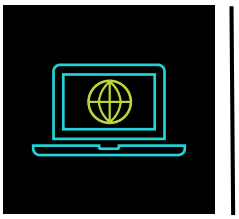
Operations of Salt Typhoon Attack Kill Chain

Salt Typhoon's tradecraft and operations consist of gaining access, establishing covert persistence, maintaining command and control, and exfiltrating valuable information from the target network. This methodology enables them to remain undetected for extended periods of time.



Initial Access

The group typically gains access through stolen credentials, supply chain compromises or exploitation of vulnerable public facing services within the telecommunications environment. In some instances, they have abused remote management systems, VPN gateways and 5G core components to bypass perimeter defenses.



Persistence

Post-compromise, the group prioritizes stealth and resilience. They use kernel-level rootkits, web shells, reverse shells, and modifications of system Dynamic Link Libraries (DLLs) and binaries are implemented to hijack legitimate services and embed into network processes to ensure their access survives reboots and endpoint security tools.

Command and Control (C2)

Salt Typhoon tends to use living-off-the-land techniques to blend their C2 traffic. This type of activity is difficult to detect from normal traffic.

Exfiltration

Rather than exfiltrate all data, the group focuses only on targeted sensitive datasets that could benefit their intelligence gathering. Call details, subscriber data, network configuration files and diagrams provide insight into military and commercial communications. Salt Typhoon often compresses, encrypts, and exfiltrates data through sharing sites.

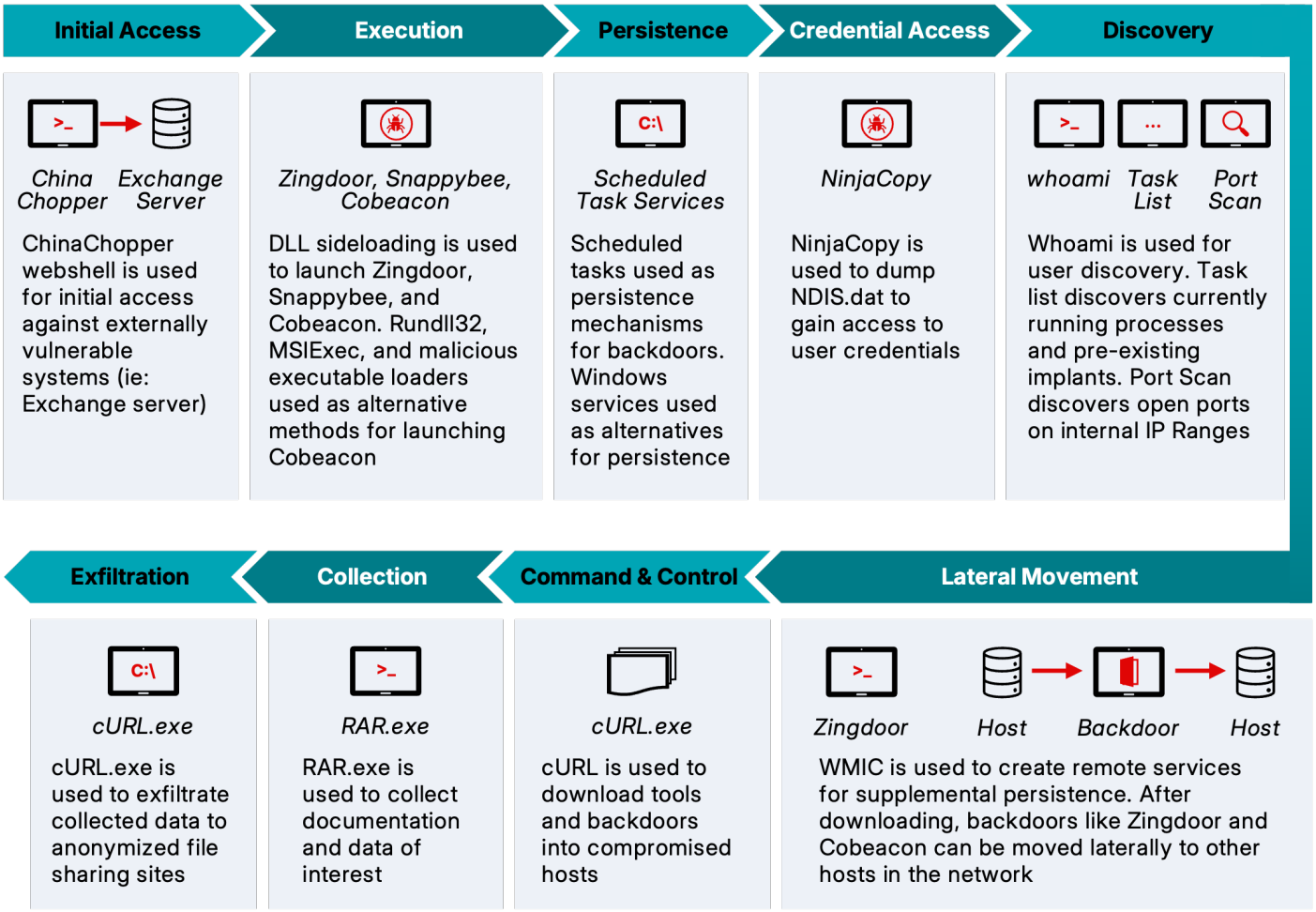


Figure 1: Salt Typhoon Attack Lifecycle Used on U.S. Critical Infrastructure

Figure 1 illustrates the Salt Typhoon attack lifecycle used to infiltrate U.S. telecommunication providers. The breach gave the attackers remote control over critical functions and allowed them to penetrate entire networks and access data. The stealth techniques the group used allowed them to maintain an undetected presence in the impacted networks for nearly 2 years, extracting Call Detail Records that included time stamps, IP addresses, phone numbers, audio recordings, and surveillance data.

Understanding Salt Typhoon: Impacts on 5G Security and Infrastructure

As the Department of War (DOW) expands 5G system use across diverse mission scenarios, a critical priority is strengthening and validating the security of these deployments, to prevent a recurrence of the Salt Typhoon attack on 5G-enabled missions. The sensitivity of the data traversing DoW 5G networks makes them an increasingly attractive target for nation-state sponsored threat actors whose primary objectives include cyber espionage, counterintelligence, and data exfiltration. These adversaries are likely to seek persistent access to 5G infrastructure, to obtain user data, intercept traffic in transit, and exploit connected devices. While all transport mediums, including 5G, carry inherent risks, the operational benefits of 5G for specific DOW mission applications far outweigh those risks, provided robust security measures and proactive threat mitigation strategies are implemented.

The Salt Typhoon campaign offered valuable insights into the TTPs employed by advanced threat actors targeting global telecommunications infrastructure. These lessons are critically important for informing mitigation strategies across current and future DOW private 5G deployments. Continuing attacks on critical infrastructure will require a secure-by-design and secure-by-default approach to effectively protect the warfighter's ability to securely communicate and perform their mission.

To translate these insights into operational terms, here are some examples that represent typical use cases for DOW 5G deployments and associated data vulnerabilities and attacks to illustrate the potential mission impacts an adversary could inflict if they were to obtain Salt Typhoon-level access to network infrastructure.

5G USE CASE	POSSIBLE IMPACTS
Asset Tracking	• Exfiltration and exposure of asset type, quantity, and location of mission critical assets • Network traffic compromise can enable eavesdropping and lateral movement within systems • Disruption of asset tracking can cause loss of asset visibility impacting mission readiness
Smart Warehouse	• Manipulation of robotics, smart sensors and automated systems can lead to malfunctions and disruptions in the workflows • Data corruption and manipulation of inventory records could prevent timely delivery of assets and disrupt operations
Flight line of the future	• Network compromise can lead to real time visibility of aircraft location or deployments • Interception or alteration of sensor and other maintenance data can be exfiltrated revealing possible vulnerabilities or other mission critical information • Falsification of logistics/maintenance records can increase downtime affecting mission success and other operations
Manufacturing	• Intrusions can disrupt production lines causing delays • Tampering of blueprints or quality control data can produce defective products, forcing rework and increasing production costs • Physical damage to equipment could be possible by manipulation through increasing usage rate

Table 1: Use Cases for DOW 5G Deployments and Associated Data Vulnerabilities and Attacks

Proactive risk reduction and targeted mitigations are essential to prevent or minimize the impact of such threats. The next section discusses continuous monitoring, zero trust adoption, secure-by-design and secure-by-default principles, and other key features.

Securing 5G Through Continuous Monitoring and Zero Trust

In 2022, Booz Allen released a white paper titled *Enabling 5G Security with Continuous Monitoring* to address one of the requirements of the fiscal year 2021 National Defense Authorization Act, which tasked the Defense Information Systems Agency and U.S. Cyber Command with developing a 5G continuous monitoring capability for non-commercial DOW networks. The paper outlined Booz Allen's perspective on how stakeholders should approach the implementation of a comprehensive continuous monitoring technology stack capable of detecting and mitigating sophisticated threats such as those posed by Salt Typhoon. The recommended approach was to implement a suite of tools and sensors, integrated with advanced analytics, to deliver visibility, alerting, and response capabilities across the entire 5G ecosystem, which includes user equipment (UEs), the radio access network (RAN), transport layers, virtualization infrastructure, and the 5G mobile core itself.

A key challenge for any continuous monitoring solution, especially in the context of 5G, is managing the immense volume, velocity, and variety of data inherent in telecom environments. At the time, applying AI and machine learning was proposed to address this complexity. That recommendation has only grown more relevant as the pace of advancement in AI capabilities has accelerated dramatically. Figure 2 illustrates the Booz Allen 5G continuous monitoring architecture, which remains highly relevant today.

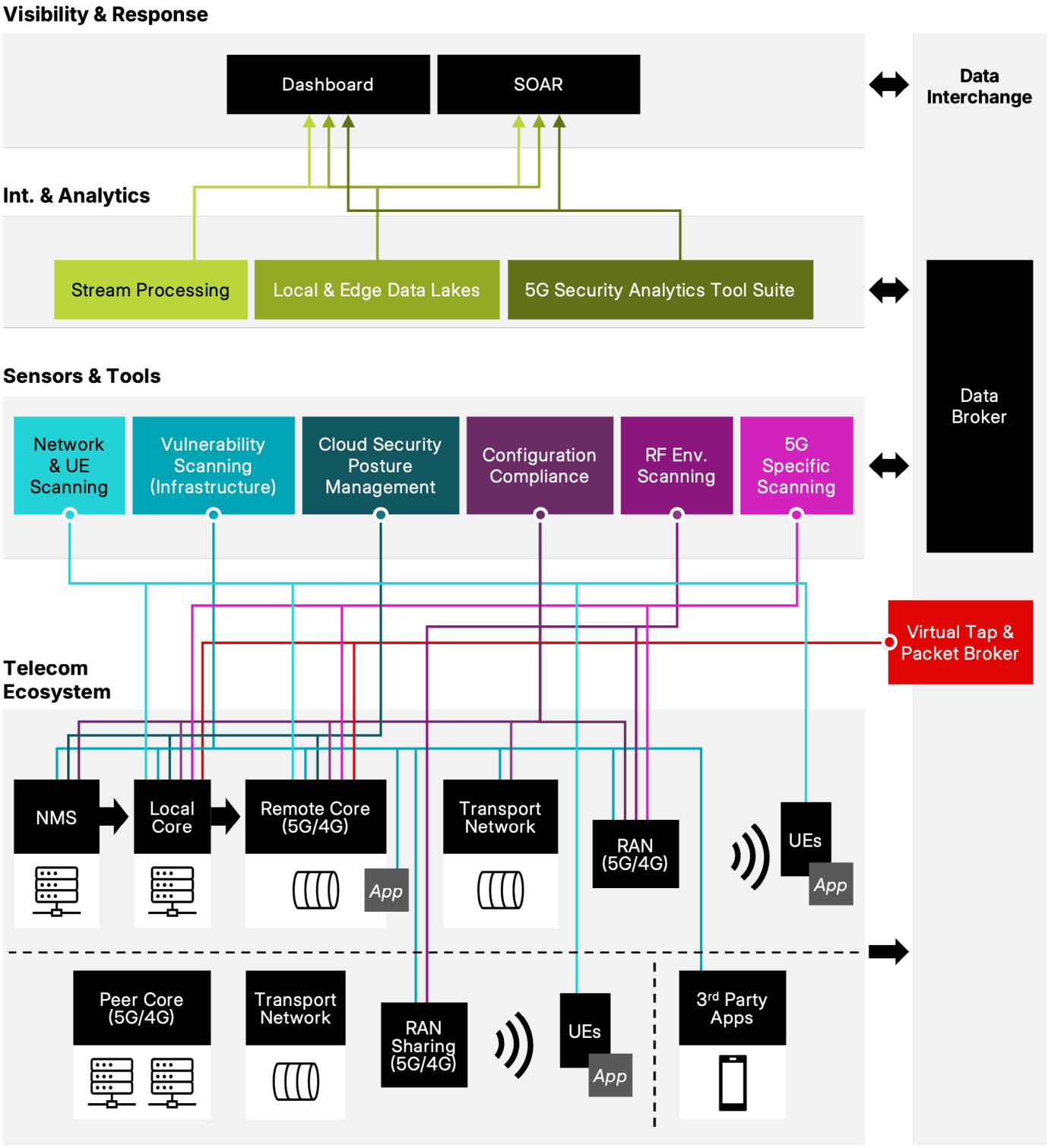


Figure 2: 5G Continuous Monitoring Architecture

Defensive Measures from Adversary Insight

The Executive Order on Improving the Nation's Cybersecurity (no. 14028) initiated sweeping government-wide efforts to ensure baseline security practices are in place, including the U.S. government's critical infrastructure, and described how a transition to a zero trust approach to security provides a defensible architecture for this new environment. Building on this directive, federal government and industry partners should now focus on reducing the attack surface of internet-exposed systems, enforcing identity and access management, and embedding secure-by-design and secure-by-default principles throughout the system lifecycles.

To illustrate how these principles can be applied, organizations can adopt a layered zero trust model that focuses on protecting the network from the core to the edge, supported by centralized management and continuous monitoring.

Secure the Core	+	Secure the Edge	+	Centralize Management
• Apply Zero Trust • Continuous Monitoring • Gain Visibility • Real-Time Threat Detection		• Single-SIM Device Isolation • Reduce Edge Attack Surface • Secure Cellular Gateway		• Unified Visibility & Control • Consistent Policy Enforcement • Streamlined Operations

Figure 3: Continuous Validation Operations

However, securing the 5G infrastructure goes beyond the architecture alone; it also needs to incorporate ongoing security operations activities that will provide constant visibility and understanding of the threat landscape after deployment.

New 5G Security Pillars

- **Risk Assessment:** Conduct a whole-system risk assessment evaluating the relevant threat landscape, reviewing system documentation (High Level Designs, Low Level Designs, etc.) and security documentation to identify the risks, and proposing mitigations for high-risk areas based on the criticality of the system elements and information
- **5G Red Teaming:** Real-world adversary tactics to test 5G network ecosystems and resiliency to reveal how advanced threats could exploit authentication gaps, misconfigurations, or supply chain weaknesses to compromise critical infrastructure
- **5G Threat Hunt:** Proactively identify, investigate, and mitigate potential threats across 5G networks by aligning threat-hunting methodologies with client-specific use cases and leveraging both traditional (e.g., firewall logs, NetFlow, endpoint detection and response logs) and emerging (e.g., subscriber session metadata, network slice telemetry, 5G core component logs) data sources to surface malicious behavior

By implementing security risk assessments, red team exercises, and threat-hunt operations, organizations ensures that defenses remain validated, security gaps are rapidly discovered and addressed and the 5G infrastructure stay resilient as the threat landscape evolves.

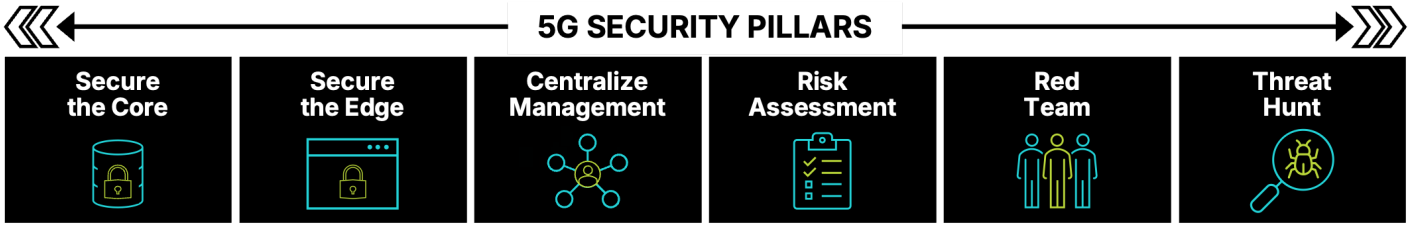


Figure 4: 5G Security Pillars

Security Capabilities for 5G Networks

While a zero trust architecture and adversary emulation operations can provide a solid understanding of the 5G infrastructure, inherent 5G technical capabilities and architecture design features can significantly enhance security posture when properly enabled. Protecting 5G networks requires a multilayered security architecture that addresses both network-specific protocols and the unique attack surfaces introduced by virtualized and software-defined environments. Modern cybersecurity platforms integrate advanced detection, segmentation, and analytics to safeguard the 5G core and edge components from exploitation.

Protocol and Traffic Protection

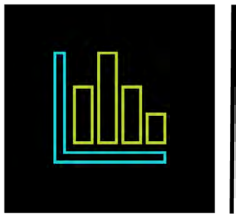
Contemporary network-defense technologies provide protection against protocol manipulation and flooding within the 5G core. They also enable policy enforcement based on mobile identity context to improve visibility and control over subscriber and device behavior.

Next-Generation Firewalls

Next-generation firewalls and security gateways are now available across multiple deployment models, such as virtual, cloud-native, and hardware-based, to accommodate various 5G use cases. This flexibility allows consistent security policy enforcement regardless of location or scale.

Cloud-Threat Intelligence

Cloud-integrated security services use machine learning and deep-learning models trained on large global datasets to identify both known and previously unseen attack patterns. These systems detect signature-based exploits, evasive or polymorphic malware, C2 activity, and techniques observed in recent nation-state campaigns, such as Salt Typhoon.



Analytics

Modern detection frameworks incorporate pre-built analytics that map to adversary TTPs documented in open frameworks such as MITRE ATT&CK. This approach ensures broad visibility across the entire intrusion lifecycle, from initial access through persistence, lateral movement, and exfiltration.

Together, these capabilities form a protective and defensive layer that mitigates some of the techniques Salt Typhoon uses. Hardening protocols and using next-generation firewalls can reduce the exposed attack surface on routers and core systems, while segmentation limits their ability to move laterally within the environment. Implementing cloud-threat intelligence and using analytics can provide visibility into exploitation chains, living-off-the-land activity that has been attributed to Salt Typhoon's or other APT operations, reducing the likelihood of data compromise and decreasing the possibility of remaining undetected.

Conclusion

The cyber threat landscape facing 5G and critical infrastructure systems continues to evolve, driving an urgency to implement defensive capabilities, strengthen cyber resiliency, and focus on secure by design deployments. As the development of NextG technology evolves, the strategies to design secure telecommunication infrastructure and defend against the rapidly accelerating threats and sophisticated adversaries of the future must evolve alongside it.

Zero trust strategies and continuous device and application monitoring have reshaped the way organizations view security. Integrating these strategies with proactive measures such as risk assessments, red team exercises, and continuous threat hunting adds a deeper layer of defense capable of evolving alongside adversary tactics. Additional mitigation is gained by emphasizing how protections within the 5G architecture, such as AI-driven monitoring and automation, behavioral analytics, machine learning models, and telemetry correlation, enable rapid threat detection with greater precision.

About Booz Allen

Booz Allen is an advanced technology company delivering outcomes with speed for America's most critical defense, civil, and national security priorities. We build technology solutions using AI, cyber, and other cutting-edge technologies to advance and protect the nation and its citizens. By focusing on outcomes, we enable our people, customers, and their missions to succeed, accelerating the nation to realize our purpose: Empower People to Change the World®.

Explore more at **www.boozallen.com/cyber**

About Palo Alto Networks

As the global AI and cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation.

Explore more at **www.paloaltonetworks.com**

Booz Allen®

BoozAllen.com