# Byos Secure Networking Platform

A National Defense Response to the Salt Typhoon Cyber Crisis

WHITE PAPER

## Executive Summary

The Salt Typhoon cyber espionage campaign, attributed to Chinese state-sponsored actors, represents one of the most significant national security threats to the United States and its allies in recent history.[1, 2] Active since at least 2021, this operation infiltrated telecommunications networks worldwide, compromising critical infrastructure and enabling long-term surveillance, data theft, and potential sabotage.[2, 3] With impacts spanning over 80 countries and affecting major U.S. telecom providers such as AT&T, Verizon, T-Mobile, Lumen, Charter Communications, Consolidated Communications, Windstream, Comcast, and Digital Reality[21]. Salt Typhoon exposed vulnerabilities in network security, leading to significant economic implications, including a $3 billion U.S. plan to remove Chinese telecom equipment, and average breach costs of approximately $4.8 million per incident for telecom firms.[2, 5]

In response to this crisis, declared a national defense emergency by U.S. authorities and international partners on August 27, 2025, the **Byos Secure Networking Platform** offerers a robust mitigation strategy.[4, 5] Designed for critical infrastructure and defense applications, Byos leverages hardware-based endpoint microsegmentation, network obfuscation via device cloaking, FIPS 140-2 validated AES-256 encryption, and multi-factor authentication (MFA) to mitigate key attack vectors exploited by Salt Typhoon. By isolating assets, preventing network discovery, blocking lateral movement, thwarting privilege escalation, and reducing persistence, Byos provides a hardware-enforced Zero Trust architecture that enhances telecommunications network resilience against state-sponsored threats, delivering targeted value to breached providers like AT&T, Verizon, T-Mobile, Lumen, and Comcast through rapid remediation and compliance support.

**This white paper presents a phased recounting of how Salt Typhoon accomplished their attack, its devastating impacts on the telecommunications sector, and how the hardware-enforced microsegmentation capabilities of Byos would have eliminated (or drastically limited) the scale and proliferation of these nation-state TTP's on layers 1-4 across the global telecommunications industry.**

## The Salt Typhoon Threat, MITRE ATT&CK, and what Byos could have done about it

### Phase 1 — Initial Access (T1190): Public-Facing Edge Exploitation

- **Observed vector**: Unauthenticated remote code execution on management Web UIs (e.g., Cisco IOS XE WebUI CVE-2023-20198), VPN gateways (Ivanti Connect Secure CVE-2024-21887/21893), and firewall portals (PAN-OS CVE-2024-3400).
- **Why it worked**: Exposed management surfaces reachable from untrusted networks; implicit trust at the physical port; coarse firewall rules; slow patch cycles on telco edge/control gear.
- Byos defense: The switch/NIC port comes up into a default-deny micro-segment; no routable IP nor L2/L3 adjacency until device identity and posture satisfy policy; management and API planes are cloaked from unauthenticated entities.

### Phase 2 — Establish Foothold (T1505.003): Web Shell / Implant

- **Observed vector**: Drop web shells or implants into edge appliances to persist across reboots, pivot, and harvest credentials.
- **Why it worked**: Once the edge device is reachable, file-system writes and daemon restarts are possible; legacy ACLs do not discriminate control-plane file ops; no first-hop guard.
- Byos defense: Out-of-band device onboarding restricts allowable flows to signed update repos and management jump hosts only; unknown write paths and inter-process calls have no egress path at the first hop.

### Phase 3 — Credential Access & Discovery (T1003/T1087/T1046)

- **Observed vector**: Loot device creds, enumerate management networks, and scan east-west for SEPP/SBC/OSS/NMS targets.
- **Why it worked**: Flat L2 domains and shared management VLANs; SNMP/SSH allowed within large address scopes; discovery traffic tolerated as 'normal'.
- Byos defense: Identity-scoped microsegments limit each asset's blast radius; east-west probes cannot traverse the first-hop policy unless explicitly allowed per role (e.g., SEPP<->SEPP over N32 with mTLS only).

### Phase 4 — Lateral Movement (T1021): Remote Services

- **Observed vector**: Pivot via SSH/RDP or appliance-to-appliance RPC toward high-value control systems (OSS/BSS/DC/NMS).
- **Why it worked**: Perimeter firewalls permit internal reachability; segmentation is policy-as-document, not policy-as-gate; credentials reuse.
- Byos defense: Per-pair allow-lists enforced in hardware at the first hop (MAC/IP/port/SNI), making unauthorized RPC or admin protocols unroutable regardless of credentials.

## Phase 5 — Collection & Exfiltration (T1041): C2/Data out

- **Observed vector**: Tunnel management data and configs over C2 channels (HTTPS/DNS/TCP), sometimes via abused signaling paths.
- **Why it worked**: Egress controls emphasize perimeter; compromised appliances are 'trusted routers' inside; signaling firewalls focus on protocol compliance, not first-hop origin integrity.
- Byos defense: Egress contracts constrain each device to named destinations (repos, management plane, telemetry sinks); anything else is dropped at the port before it becomes a 'network' problem.

## Phase 6 — Defense Evasion & Persistence (T1070/T1547)

- **Observed vector**: Modify startup configs, rotate implants, and live-off-the-land to survive patch/upgrade cycles.
- **Why it worked**: Change control assumes the right admin is on the right box; device-local controls can be bypassed once root is obtained.
- Byos defense: Tamper-resistant out-of-band orchestration with signed policy; one-click isolation removes the asset from all adjacencies while retaining operator access through a break-glass path.

| Stage | Description | Technical Details and Examples | Byos Countermeasures |
|---|---|---|---|
| **Initial Access** | Exploits known vulnerabilities in public-facing network devices and endpoints, often due to delayed patching. | • Targets routers, firewalls, and VPN gateways.<br>• Key CVEs: Ivanti Connect Secure (CVE- 2024-21887), Palo Alto PAN-OS (CVE- 2024-3400), Cisco IOS XE (CVE-2023-20198 chained with CVE- 2023-20273).<br>• Uses double-encoded requests and scans for high-port SSH services (e.g., ports ending in '22' like 57722). | Byos' hardware-based endpoint microsegmentation isolates devices into individual segments, making them invisible to external scans via network obfuscation and device cloaking.<br><br>FIPS 140-2 validated AES-256 encryption secures all ingress/egress traffic, while MFA enforces strict access controls, preventing unauthorized exploitation of vulnerabilities. |
| **Persistence and Privilege Escalation** | Modifies configurations to maintain long-term access while remaining stealthy. | • Alters access control lists (ACLs) and creates privileged accounts.<br>• Enables remote management on nonstandard ports (e.g., activating IOS XR SSH listener on port 57722).<br>• Deploys custom tools detected by YARA rules; uses Snort rules for spotting malicious escalation attempts.<br>• IP addresses traced back to 2021 for command-and-control. | Byos reduces persistence by operating OS independently with decoupled security, zeroizing unauthorized modifications.<br><br>Privilege escalation is thwarted through least-privilege enforcement, granular microsegmentation, and hardware-enforced MFA, ensuring attackers cannot create or exploit elevated accounts. |
| **Lateral Movement and Pivoting** | Moves across networks to expand reach, leveraging compromised systems as footholds. | • Pivots to adjacent devices and harvests administrator credentials from TACACS+ packets.<br>• Mirrors network traffic using SPAN, RSPAN, or ERSPAN to monitor communications without alerting users.<br>• Lateral movement is subtle, often undetected by traditional security tools as it blends with legitimate traffic. | Byos blocks lateral movement via endpoint isolation in microsegments, preventing pivoting between devices.<br><br>Network obfuscation hides assets, while AES-256 encryption and MFA protect credential harvesting, limiting the blast radius and ensuring threats cannot propagate. |
| **Data Collection and Exfiltration** | Steals sensitive data while minimizing footprints. | • Captures packets with suspicious names (e.g., 'tac.pcap').<br>• Exfiltrates via GRE and IPsec tunnels designed to appear as normal data flows.<br>• Focuses on call records, emails, texts, and metadata for surveillance; enables real-time monitoring of targeted individuals. | Byos secures data flows with end-to-end FIPS-validated encryption, detecting and blocking anomalous exfiltration.<br><br>Microsegmentation and obfuscation prevent traffic mirroring, while centralized management with MFA ensures only authorized access, neutralizing surveillance attempts. |
| **Overall Tradecraft** | Relies on custom malware and tools for sabotage potential, embedded in critical systems like energy and transportation. | • Pre-positions capabilities for disruption (e.g., delaying military ops or causing outages).<br>• Uses hybrid-cloud exploits for privilege escalation across environments. | Byos' agentless, CSfC-compliant architecture, combined with ITAR compliant hardware, counters tradecraft through comprehensive Zero Trust. Features like device hardening, secure-by-design principles, and anti-lateral-movement technology mitigate embedded threats, providing robust defense for telecom and critical infrastructure. |

## Impacts on the Telecommunications Industry

The telecommunications sector, serving as the backbone of global communications, has borne the brunt of Salt Typhoon's intrusions.[1, 3] At least nine major U.S. carriers, including AT&T, Verizon, T-Mobile, Lumen, and Comcast, have been compromised, exposing nearly every American's cellular communications and leading to widespread data theft.[2, 3, 5] Financial impacts include:

- **Direct Costs**: Remediation, patching, and audits, with broader implications leading to a $3 billion U.S. plan to remove vulnerable Chinese telecom equipment; average per-incident costs in telecom reach ~$4.8 million, encompassing forensic investigations and system upgrades, as experienced by providers like AT&T and Verizon.[6]
- **Indirect Losses**: Reputational damage, regulatory fines (e.g., akin to T-Mobile's $92 million FCC penalty), and legal liabilities from data breaches, affecting sectors like healthcare and energy, with companies like Lumen and Comcast facing additional scrutiny over broadband and data center integrations.[2, 5]
- **Broader Economic Ripple**: Disruptions could lead to widespread losses for reliant industries, including service outages, misrouted emergency calls, supply chain delays in 5G rollouts, and eroded trust in communications, particularly impacting large-scale operators like Verizon and AT&T with their extensive customer bases.[1]

These vulnerabilities highlight the need for proactive, hardware-enforced solutions like Byos, which can mitigate such exploits at the edge, ensuring secure connectivity even on untrusted networks.

## Compromise of CALEA Lawful Intercept (Wiretap) Operations

Multiple government and media reports indicate that Salt Typhoon breached "lawful intercept" systems at several U.S. telecommunications providers—the infrastructure used to process court-authorized wiretap requests under the Communications Assistance for Law Enforcement Act (CALEA).[18]

By accessing systems that house active wiretap requests and surveillance data, the attackers jeopardized ongoing criminal and counterintelligence investigations and, potentially, lives—given the risk of suspects being tipped off or operations being compromised.[19]

Byos containment relevance: lawful-intercept mediation devices and related LI controllers should be placed into hardware-enforced first-hop microsegments with default-deny adjacency, device cloaking, and destination pinning to approved collection points only. This prevents LI management planes and mediation interfaces from being discovered or reached by compromised assets, and ensures that any data export paths are cryptographically bound to explicit policies.[20]

## Hypothetical Case Studies: Mitigating Neer-Peer Threats in Telecom Environments

To illustrate Byos' efficacy, consider the following hypothetical scenarios based on Salt Typhoon's known targeting of U.S. and allied partner telecommunications threat surface:

### Signaling & Interconnection Protection (SEPP/SBC/STP/DEA)

- **Problem**: Inter-PLMN and interconnect signaling is often reachable from semi-trusted partners who themselves might be compromised; protocol conformance checks alone cannot stop source-spoofed, topology-probing abuse.
- Byos Solution: First-hop contracts restrict each signaling node (SEPP/SBC/STP) to exact peer identities and reference points (e.g., N32), with mTLS requirements and topology hiding enforced before IP routing.

### Edge & Access Network Appliances (Routers, vBNG, CGNAT, Firewalls)

- **Problem**: Edge devices expose management surfaces (WebUI/SSH/SNMP) and APIs; once compromised, they become privileged pivot points.
- Byos Solution: Port-up default-deny with per-role egress; management reachable only via bastions; update traffic pinned to vendor CRLs and signed repos.

### OSS/BSS & NMS/EMS Isolation

- **Problem**: Operational systems often reside on shared management VLANs with broad reach, enabling reconnaissance and credential replay.
- Byos Solution: Micro-segments per application tier; break-glass isolation to contain suspected compromise while keeping operator access.

### Emergency Services (E911/NG911/MCX)

- **Problem**: Mission-critical call routing and PSAP interfaces demand deterministic paths and cannot tolerate lateral threat movement.
- Byos Solution: Hardware-anchored path control and destination pinning; deterministic fail-safe isolation without black-holing emergency traffic.

### Roaming & Peering Facilities (IXPs, Core Sites)

- **Problem**: Multi-tenant co-los with complex cross-connects expand the attack surface.
- Byos Solution: First-hop identity before cross-connect activation; scoped peer adjacency with cryptographic binding.

### Telecom Signaling & Interconnection Infrastructure (SS7, Diameter, SIP, and Peering Links)

- **Problem**: Telecom networks rely on legacy signaling protocols (SS7 for 2G/3G, Diameter for 4G, SIP for VoIP/5G) and interconnection/peering agreements between carriers. These signaling paths are high-value espionage targets (Salt Typhoon already exploited SS7/Diameter). They often remain flat and trusted, with weak authentication, making them vulnerable to:
  - IMSI catchers & location tracking
  - Metadata harvesting (call/SMS records, subscriber data)
  - Rogue redirection of calls/SMS (SIM swap support, wiretap bypass)
  - Abuse of lawful intercept gateways
- Byos Solution
  - Hardware Microsegmentation: Each signaling node (HLR, HSS, MSC, IMS Core) is isolated into its own secure microsegment. Even if one node is compromised, attackers cannot pivot laterally to others.
  - Device Cloaking: Byos hides SS7/Diameter/SIP servers from reconnaissance, making them invisible to external scans and unauthorized peer carriers.
  - Zero-Trust Outbound Enforcement: Byos policies allow only approved interconnection traffic (e.g., SIP to specific peering partners), blocking covert tunnels or unauthorized signaling flows.
  - FIPS-Validated Encryption: Metadata carried over insecure interconnects can be wrapped in Byos' AES-256 overlay, protecting against surveillance and tampering.
  - Resilient Management Isolation: Byos ensures signaling management interfaces (often Internet-exposed for remote vendors) are cloaked and only accessible through secure overlay sessions.
- **Real-World Value**
  - Protects hybrid 4G/5G deployments where legacy SS7/Diameter coexist with modern signaling.
  - Helps telecoms comply with CISA's 2023/2025 telecom guidance to "isolate management planes and enforce multi-factor access controls."
  - Aligns with NTIA Innovation Fund goals: Byos could be deployed as part of secure open RAN testbeds, ensuring signaling resiliency for interoperable 5G networks.
  - Strengthens resilience at carrier interconnect points — critical for national security and continuity of emergency services (E911, FirstNet).

These problems are universal in global telecommunications networks today. With the Byos Secure Networking Platform deployed on your network, they become yesterday's problems.

## Byos: Enhancing US and Allied Telecommunications Security

Salt Typhoon's global reach, affecting telecommunications in over 80 countries, underscores the interconnected nature of cyber threats to the US and its allies.[3] Allied intelligence agencies, including those from the Five Eyes (US, UK, Canada, Australia, New Zealand) and partners like Germany, Spain, and Japan, have collaborated on attributions and defenses, highlighting the need for shared cybersecurity tools in telecom infrastructure.[2] From a telecommunications perspective, Byos can play a pivotal role in bolstering collective defense by securing cross-border communications, enabling secure data sharing, and preventing espionage that could undermine joint military operations or economic alliances.

Byos' made-in-USA, ITAR-compliant hardware ensures it meets export controls while being deployable to trusted allies, fostering interoperability in multinational telecom networks.[10] For instance, its Zero Trust architecture, with features like network obfuscation and encrypted remote access, protects shared infrastructure—such as undersea cables or satellite links—against infiltration, reducing risks of global surveillance norms violations.[4] In alliances like NATO or AUKUS, Byos can secure OT/IoT devices in joint exercises, ensuring resilient comms for real-time intelligence sharing without exposing vulnerabilities.[15] By isolating threats at the edge and providing granular access controls, Byos helps prevent cascading effects from breaches in one ally's network to

others, strengthening overall alliance cyber posture and supporting initiatives like the US-UK Cyber Dialogue on telecom security.[6] Ultimately, adopting Byos across allied telecom sectors promotes a unified front against state-sponsored actors, enhancing global democracy and stability by safeguarding the digital backbone of international cooperation.[6]

## Competitive Analysis

Byos differentiates itself in the microsegmentation and Zero Trust space through its hardware-based, agentless approach, ideal for telecom's legacy and OT devices. Our Secure Networking Platform can integrate with and improve upon industry-leading solutions, making it a capex-lite accelerator to the security posture of telecommunications companies worldwide. Extending your current investments with Byos enables you to defend what other solutions only observe:

- **Illumio**: Excels in software-defined network microsegmentation with strong support ratings (9.5/10 on TrustRadius), but its agent-based approach complicates deployment on diverse telecom hardware like base stations or legacy routers.[15]
  - Byos Improvement: Byos' agentless endpoint microsegmentation architecture simplifies integration across heterogeneous telecom environments, reducing deployment time by up to 30% (based on similar OT deployments), which is critical for rapid response to Salt Typhoon's persistent threats in networks like T-Mobile's 5G infrastructure.[11, 12]
- **Zscaler**: Provides cloud-based Zero Trust with high efficacy in web security, but user reviews note lower support ratings (8.9/10) and potential latency in high-throughput telecom scenarios (e.g., 100Gbps links).[2]
  - Byos Improvement: Byos' on-premise, hardware-enforced solution minimizes latency for edge computing—essential for Comcast's broadband services—while offering FIPS 140-2 validated encryption (Certificate #4946) for compliance with stringent regulatory requirements, unlike Zscaler's cloud-first model.[11, 12, 13]
- **Cisco Secure Access**: Integrates seamlessly with Cisco ecosystems prevalent in telecom networks, offering superior latency and connections.[3, 6] However, as a software/service edge (SSE) solution, it lacks robust hardware-enforced obfuscation for legacy protocols like SS7, potentially leaving gaps in hybrid 4G/5G networks.[3, 6]
  - Byos Improvement: Byos enhances Cisco's capabilities by providing hardware-based obfuscation and microsegmentation, protecting vulnerable signaling protocols and reducing the attack surface in hybrid environments, which is vital for Verizon and AT&T's extensive Cisco deployments.[11, 12]
- **CrowdStrike Falcon (EDR/XDR)**: Falcon Insight XDR provides endpoint detection and response with network containment (host isolation) and AI-driven telemetry correlation across domains. In telco implementation, it has blind spots for unmanaged/legacy/OT network assets without agents; lateral movement can occur over L2/L3 paths before containment triggers; reliance on OS integrity
  - Byos Improvement: Byos enforces first-hop isolation to shrink the blast radius; agentless microsegmentation brings zero-trust access at the wire; Byos tags can trigger Falcon containment and streamline DFIR.
- **Palo Alto Networks (Prisma Access / ZTNA 2.0 / NGFW)**: Prisma Access (SSE) and ZTNA 2.0 deliver cloud-delivered secure access and continuous inspection; PAN-OS NGFWs secure perimeters/data centers. In telco implementations, its inline controls often start at the routing perimeter; unmanaged assets on L2 segments and remote jump hosts can still be discoverable; firewall/SD-WAN policies don't granularly enforce first-hop control per device.
  - Byos Improvement: Byos edges enforce hardware-first segmentation at the NIC, making assets invisible on local segments and steering traffic to Prisma/NGFWs by policy—raising efficacy without major redesign.

Byos excels in critical infrastructure with its focus on invisibility and isolation, complementing existing telecom ecosystems while addressing specific gaps in competitor solutions.

## Byos Secure Networking Platform: The Solution Explained

The Byos Secure Networking Platform is engineered for the most demanding operational environments, including defense and critical infrastructure, offering a made-in-USA, ITAR-compliant solution that aligns with DoD's Cybersecurity Maturity Model Certification (CMMC). Its core capabilities ***directly counter Salt Typhoon's tactics***, with telecom-specific integrations delivering value to providers (like AT&T, Verizon, T-Mobile, Lumen, and Comcast) by securing vast subscriber networks and hybrid infrastructures:

- Endpoint Microsegmentation: Hardware-enforced isolation creates individual network segments for each device, preventing discovery and lateral movement. This collapses the attack surface, ensuring compromised endpoints cannot pivot or propagate threats, and integrates with ETSI NFV standards to protect 5G core functions—crucial for T-Mobile's rapid 5G expansions.[11, 12]
- Network Obfuscation: Through device cloaking and invisibility on local networks, Byos hides assets from reconnaissance, rendering Salt Typhoon's scanning and fingerprinting ineffective—particularly useful for obscuring SS7/Diameter signaling paths in legacy 4G, aiding Lumen's enterprise connectivity services.[11, 12]
- FIPS 140-2 Validated AES-256 Encryption: All communications are protected with CNSA 2.0- approved, certified encryption (Certificate #4946), securing data in transit and at rest against interception and exfiltration, including metadata from telecom protocols—essential for Comcast's broadband and media integrations.[12, 13]

- Multi-Factor Authentication (MFA): Hardware-enforced MFA, integrated with Zero Trust principles, prevents unauthorized assets from gaining access, or achieving privilege escalation, requiring multiple verification factors for any network interaction, enhancing protection for admin access in SDN/NFV stacks used by Verizon and AT&T.[11, 12]

Additional features, such as agentless deployment, OS-independence, centralized management via Byos Secure Lobby™, and protection for OT/legacy devices, further reduce persistence by enabling rapid threat isolation and eviction without disrupting operations. In telecom contexts, Byos secures untrusted connections, ensuring resilient data flows amid state-sponsored attacks, with compatibility for tools like Splunk for IOC hunting—providing scalable solutions for the massive traffic volumes handled by these major providers.[11, 12]

*CISA's Zero Trust Maturity Model (2023) explicitly recommends* hardware-based security measures, such as endpoint detection and response (EDR) and secure access controls, to protect critical infrastructure like telecom networks[5]. The August 27, 2025, joint advisory on Salt Typhoon emphasizes isolating management planes and enforcing MFA, which aligns with hardware-enforced Zero Trust principles[13]. CISA's guidance supports solutions like Byos, which use hardware-based microsegmentation and encryption to prevent unauthorized access and persistence.[14]

## Conclusion

Salt Typhoon exemplifies the evolving cyber threats facing national security, demanding immediate adoption of advanced defenses.[1] The Byos Secure Networking Platform provides a comprehensive mitigation strategy, empowering telecommunications providers like AT&T, Verizon, T-Mobile, Lumen, and Comcast to address these risks. By deploying Byos, organizations can achieve proactive protection, compliance with defense standards, and a fortified posture against future APTs.

## Actionable Steps for Telecom Decision Makers:

- Assess Exposure: Audit edge devices for CVEs and monitor for anomalous traffic mirroring.
- Pilot Byos: Deploy in a test environment focusing on legacy 4G signaling protection.
- Calculate ROI: Compare deployment costs against potential $4.8M breach losses.
- Contact for Demo: Reach out to Byos for a customized telecom assessment tailored to your network, such as AT&T's or Verizon's infrastructure.

For more information or to see a demo, visit byos.io
or email us at engage@byos.io

# Appendix A: References


1. CISA. "CISA and Partners Release Joint Advisory on Countering Chinese State-Sponsored Actors' Compromise of Telecommunications Infrastructure." Aug 27, 2025. https://www.cisa.gov/news-events/news/cisa-and-partners-release-joint-advisory-countering-chinese-state-sponsored-actors-compromise
2. FBI/CISA/NSA et al. "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide." Cybersecurity Advisory, Aug 27, 2025. https://www.ic3.gov/CSA/2025/250827.pdf
3. NSA. "Guidance to Counter China State-Sponsored Actors Targeting Telecommunications and Other Sectors." Press Release, Aug 27, 2025. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4287371/
4. Reuters. "International coalition calls out Chinese companies over Salt Typhoon campaign." Aug 27, 2025. https://www.reuters.com/business/media-telecom/international-coalition-calls-out-three-chinese-companies-over-hacking-campaign-2025-08-27/
5. DoD CIO. "Cybersecurity Maturity Model Certification (CMMC) – Program & Model Overview." https://dodcio.defense.gov/CMMC/
6. Forbes. "U.S. And Allies Declare Salt Typhoon Hack A National Defense Crisis." Aug 30, 2025. https://www.forbes.com/sites/emilsayegh/2025/08/30/us-and-allies-declare-salt-typhoon-hack-a-national-defense-crisis/
7. IBM/Ponemon. "Cost of a Data Breach 2025." July 30, 2025. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications-97-of-which-reported-lacking-proper-ai-access-controls
8. Cisco PSIRT. "Multiple Vulnerabilities in Cisco IOS XE Web UI – CVE-2023-20198, CVE-2023-20273." https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
9. Ivanti. "CVE-2024-21887 Command Injection (ICS/IPS)." https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways
10. Palo Alto Networks. "PAN-OS GlobalProtect Vulnerability CVE-2024-3400." https://security.paloaltonetworks.com/CVE-2024-3400
11. NIST SP 800-207. "Zero Trust Architecture." 2020. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf
12. CISA. "Zero Trust Maturity Model Version 2.0." April 2023. https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf
13. ENISA. "Signalling Security in Telecom SS7/Diameter/5G." March 2018. https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g
14. GSMA. "5GS Roaming Guidelines (NG.113) v12.0." 2025. https://www.gsma.com/newsroom/wpcontent/uploads/NG.113-v12.0.pdf
15. NIST CMVP. "FIPS 140-2 Certificate #4946 – Byos OpenSSL FIPS Provider (Level 1)." Feb 12, 2025. https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4946
16. CrowdStrike. "Falcon Insight XDR – Network Containment." https://www.crowdstrike.com/en-us/platform/endpoint-security/falcon-insight-xdr/
17. Palo Alto Networks. "Prisma Access & ZTNA 2.0." https://www.paloaltonetworks.com/sase/access
18. Nextgov/GovExec (Apr 24, 2025): FBI asks public for tips; article notes Salt Typhoon breached several U.S. telecoms' lawful intercept systems that house wiretap requests. https://www.nextgov.com/cybersecurity/2025/04/fbi-asks-public-tips-about-salt-typhoon-telecom-hacks/404814/
19. Reuters (Nov 13, 2024): U.S. authorities said China-linked hackers intercepted surveillance data intended for American law enforcement after breaking into telecoms. https://www.reuters.com/technology/cybersecurity/china-affiliated-actors-compromised-networks-multiple-telecom-companies-us-says-2024-11-13/
20. EPIC summary (Jan 17, 2025): FCC NPRM launched to secure CALEA lawful intercept systems in response to Salt Typhoon. https://epic.org/fcc-initiates-rulemaking-to-secure-government-wiretap-system-in-response-to-salt-typhoon-breach/
21. https://breached.company/salt-typhoon-chinese-hackers-expand-beyond-telecom-to-target-critical-us-data-infrastructure/