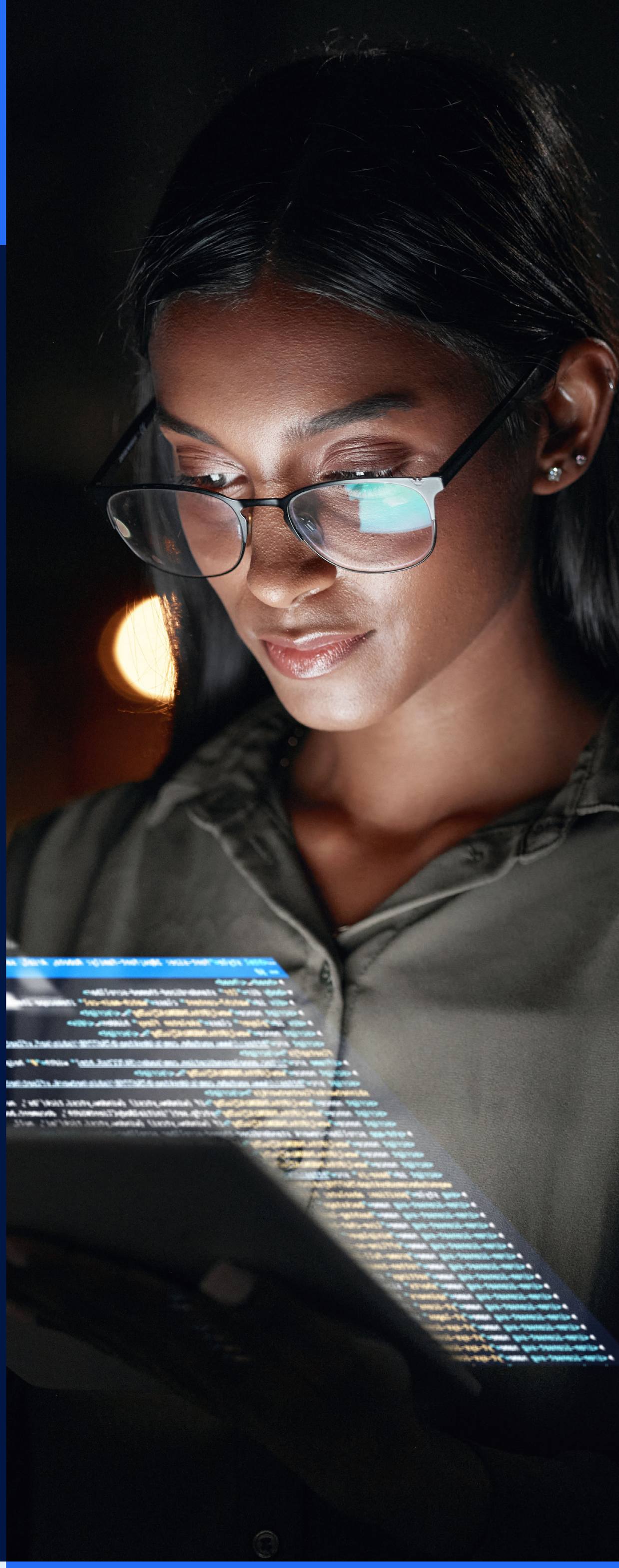
Securing the Operational Lifeline: Zero Trust for Out-of-Band (OOB) and Lights-Out Management

From Unchecked Exception to an ‘Island of One’ Microsegment: The Zscaler Cellular Architectural Shift.

This paper explains why legacy OOB designs create routable backdoors and how Zscaler Cellular turns each OOB endpoint into an isolated ‘island of one.’



WHITEPAPER

Executive Summary

Critical infrastructure operators face an uncomfortable reality: outages and cyber incidents rarely arrive one at a time. When primary connectivity is degraded, segmented, or unavailable, teams still need a trusted way to diagnose, recover, and restore operations across remote sites. In those moments, out-of-band (OOB) connectivity and lights-out management become the operational lifeline.

However, the same recovery path is often engineered as a high-privilege bypass. OOB networks are frequently routable, protected by shared or long-lived credentials, and excluded from the inspection, segmentation, and governance applied to in-band administrative access. This creates a Tier-0 control plane that is reachable when everything else is locked down, and too often under-monitored when it matters most. The impact is not theoretical: compromise of lights-out access can enable persistent control, firmware-level manipulation, and rapid expansion of blast radius across distributed environments.

Traditional designs such as VPN concentrators, private APNs, static allowlists, and jump hosts emphasize network reachability over identity-centric control. Once a user or device is "on the network," implicit trust can creep in. That makes it difficult to enforce least privilege, prevent lateral movement, and generate consistent audit evidence across remote sites and heterogeneous operational environments.

Zscaler secures OOB and lights-out management by applying Zero Trust to cellular connectivity, treating it as an enforcement point rather than just a transport. With Zscaler Cellular, OOB traffic is steered through the Zscaler Zero Trust Exchange, where access is granted only through explicit policy based on identity, device posture, application or service, and context. This approach reduces routability, limits reach to approved management interfaces, and applies consistent inspection and logging without relying on broad network access or brittle site-by-site configurations.

For critical infrastructure, the outcome is a safer recovery path and a more resilient operating model: secure remote administration during outages, reduced exposure of Tier-0 assets, simplified policy across distributed locations, and auditable controls aligned to Zero Trust principles. This paper explains why legacy OOB approaches fall short, defines the requirements for modern OOB security, and provides a reference approach for implementing "islands of one" protection for lights-out management using Zscaler.

The OOB Paradox: Operational Imperative vs. Uncontrolled Risk

Critical infrastructure environments fail in ways that undermine the controls security teams depend on. Links go down. Segments isolate. On-site access is delayed. Visibility becomes partial. Yet operations must continue, and responders still need a trusted path to diagnose, recover, and restore services across remote locations. This is the out-of-band (OOB) paradox.

OOB and lights-out management exist to preserve availability under adverse conditions, but they are often implemented as a parallel access plane that is easier to reach and harder to govern than in-band administration. Over time, what begins as "break-glass" becomes routine access, and what was meant to reduce downtime becomes a persistent high-privilege exposure.

From a Zero Trust perspective, the risk is not that OOB exists. The risk is that many OOB designs prioritize reachability over control: routable access paths, broad network-level trust, long-lived credentials, and inconsistent inspection and logging. That combination turns OOB into a Tier-0 control plane. If an adversary gets in, they can bypass endpoint controls, outlast reimages, and move laterally through management interfaces that were never meant to be broadly reachable.

Energy and Utilities

Substation recovery becomes a foothold

A utility loses in-band connectivity to a remote substation during an outage. Teams pivot to cellular OOB to access routers, firewalls, or management controllers and restore operations. If the OOB path is broadly reachable or protected with static allowlists and long-lived credentials, an attacker who gains access can persist in the management plane and regain control even after systems are rebuilt.

Manufacturing and Industrial

Vendor support expands beyond intended access

A plant authorizes a vendor to troubleshoot equipment via OOB to reduce downtime. The access is meant to be limited and time-bound, but network-based constructs (VPN/APN rules) often grant broader reach once connected, and exceptions linger. If the vendor identity is compromised, the attacker inherits that same reach across high-privilege management interfaces.

Technology (Platforms/SaaS)

Respond depends on an access path security can't govern

During a major incident impacting a cloud app stack (e.g., Salesforce or Microsoft 365), responders often fall back to break-glass or out-of-band access—jump hosts, emergency VPNs, bastion accounts, or direct console access—when primary connectivity or tooling is degraded. After recovery starts, security teams struggle to reconstruct who used that path, from what device, what systems were reachable, and what actions were taken. Because OOB is typically designed for reachability first, governance and visibility are inconsistent, leaving fragmented logs and limited inspection that weaken containment, slow forensics, and create audit gaps.

The details vary by industry, but the underlying pattern is consistent: when OOB is designed for reachability first, it becomes a high-privilege pathway that is difficult to govern and easy to misuse.

A prime example of this transformation comes from a leading consulting firm that faced growing challenges with their legacy OOB operations. Despite adopting cellular connectivity, reliance on public internet and Private APNs led to fragmented visibility, operational complexity, and heightened exposure to emerging threats. Regulatory requirements including Zero Trust mandates from authorities like the ACSC made a robust shift essential. By adopting Zscaler Cellular, the firm replaced cumbersome architectures with a secure-by-design solution that delivered granular traffic control, centralized oversight, and resilient, always-on connectivity. Combined with Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA), Zscaler Cellular reinvented their OOB access into a secure, scalable architecture defined by simplicity, resilience, and the agility needed to support evolving business demands

The common root cause: OOB is treated as connectivity, not as a Tier-0 access plane

Across industries, OOB is frequently built around making remote sites reachable. That mindset creates implicit trust once connectivity is established, and it makes least privilege difficult to express and enforce. A Zero Trust approach flips the model: access is granted to a specific management interface based on verified identity and context, not because a network path exists. A modern OOB strategy starts by changing the question from “How do we reach the site when it is down?” to “How do we ensure only the right identity can reach only the right management interface, under the right conditions, with full inspection and audit?” This is where cellular-native Zero Trust enables an “island of one” model, reducing routability and replacing exception-driven connectivity with explicit, policy-controlled access.

Hidden Exposure: The Tier-0 Control Plane Most Organizations Underestimate

OOB and lights-out interfaces were designed for reliability, not adversarial conditions. In critical infrastructure, that reliability makes them indispensable. It also makes them attractive targets. These interfaces often provide direct, privileged control over systems that underpin safety, uptime, and service continuity.

The hidden exposure is not simply that OOB exists. It is that OOB frequently operates as a parallel administrative plane with weaker controls than in-band access. Many organizations cannot quickly answer foundational governance questions: Which assets have lights-out interfaces enabled? Who can reach them? Under what conditions? How is access monitored, approved, and revoked?

From a threat perspective, compromise of lights-out access can enable actions that bypass conventional controls. Attackers can gain console-level control, change boot settings, manipulate firmware, disable security tooling, or persist below the operating system. Even strong endpoint protection cannot compensate if the management plane itself is broadly reachable and over-privileged.

What leaders should take away: Treat OOB and lights-out as Tier-0 assets. They require the same rigor as identity systems and core network infrastructure: explicit access policy, least privilege, continuous verification, and audit-grade visibility.

Navigating the Complex Security Landscape of OOB / Lights-Out Management

The modern enterprise is defined by complexity, driven by the expansion of distributed operations across Critical National Infrastructure (CNI), vast retail networks, and industrial IoT deployments. Managing these geographically dispersed assets and ensuring continuous operational uptime is paramount to business continuity and shareholder value. This operational reality is why OOB and Lights-Out Management (LO) have evolved from an IT convenience into an operational imperative.

OOB functions as the mission-critical lifeline, guaranteeing remote recovery and administration of high-privilege infrastructure components, particularly when primary in-band connectivity fails. However, this essential operational need creates a fundamental security dilemma. Traditional OOB enablement models relying on VPNs, extended private networks, or carrier APNs violate Zero Trust principles by establishing unchecked exception paths. These paths bypass core enterprise security controls, making them prime vectors for attackers and exposing high-privilege control planes.

For CIOs and CISOs seeking to harmonize operational resilience with a Zero Trust posture, the challenge lies in governing these access paths. Enterprises must confront four systemic pain points inherent in legacy OOB approaches

Top Enterprise Challenges

Unmanaged Control Planes and the Violation of Least-Privilege Access

OOB management interfaces inherently function as the highest-privilege "control planes" for an organization's core infrastructure. By design, they are empowered to manage critical systems like servers, network devices, and power distribution units (PDUs). The core Zero Trust principle dictates that access must be explicitly verified and granted with the least necessary privilege; yet, traditional OOB access often grants broad network reach based on a perimeter-centric assumption.

A compromise of this OOB control plane is a high-impact event, allowing an attacker to execute:

- Remote console access and credential capture
- Firmware or BIOS modification to establish persistence
- Network reconfiguration or full system takeover that bypasses intact endpoint agents and OS controls

The result is an immediate, high-impact security risk where a single point of failure grants total system control.

System Heterogeneity and the Complexity of Consistent Policy Enforcement

OOB environments are rarely uniform, compounding the difficulty of applying a unified security strategy. Enterprises must manage a heterogeneous ecosystem that includes:

- Server management controllers (e.g., iDRAC, iLO, IPMI–based platforms)
- Network management capabilities (console servers, dedicated management ports)
- Power infrastructure (smart PDUs, UPS management cards)
- A range of edge compute and hyperconverged stacks

Each component utilizes distinct management protocols, authentication methods, and is governed by long–lifecycle firmware with inconsistent patch cadences. This diversity creates significant operational complexity for security teams attempting to implement consistent controls, audit access, and govern permissions across multiple sites and vendor ecosystems.

Operational Reach in Remote Sites with Minimal Security and Visibility

OOB's primary use case guaranteeing connectivity to the most dispersed and lightly staffed locations (e.g., utility substations, retail branches) is exactly where security vulnerabilities are amplified. These sites often lack the standard security rigor of a corporate headquarters:

- **Weak Physical Controls:** Remote data cabinets and kiosks often lack 24/7 security or robust access systems, making the OOB pathway susceptible to physical compromise or insider threat.
- **Inconsistent Network Design:** To reduce cost, network segmentation is frequently minimal or absent. The high–privilege OOB management network often shares segments with less–secure operational or general user networks, creating a broad, low–friction attack surface that bypasses traditional perimeterdefenses.
- **Third–Party Exposure:** Essential troubleshooting frequently requires deep access for Managed Service Providers (MSPs) and vendors. Without a Zero Trust framework, granting this access often becomes an all or–nothing proposition, unnecessarily exposing the entire remote environment to external parties.

This environment of operational necessity combined with security vulnerability frequently leads to "shadow IT" access temporary emergency bypasses or vendor access links that become permanent, persistent, and unmonitored.

Architectural Flaws in Legacy Access Models Expand the Routable Attack Surface

The prevailing reliance on traditional access models particularly for cellular connectivity used in OOB is an architectural flaw that actively undermines Zero Trust initiatives. These models were designed around perimeter defense, which is ill-suited for mobile, distributed infrastructure.

The three most common legacy models introduce specific risk vectors:

- **Direct-to-Internet Access (Model A):** Provides minimal inline security, weak visibility, and makes it challenging to enforce consistent enterprise access policies.
- **Private APN/Backhaul (Model B):** Extends the enterprise network perimeter to the cellular edge, creating routable paths that facilitate lateral movement across what become flat networks once an attacker gains initial access.
- **VPN-based Access (Model C):** Expands the blast radius for credential theft, encourages broad network reachability, and complicates multi-party access governance, often resulting in persistent, overprivileged access granted for mere operational convenience.

Across all traditional methods, security teams lack the consistent, global visibility and inline control necessary to enforce least-privilege access, especially when OOB spans multiple carriers and geographies.

The Zscaler Cellular Architectural Shift: Extending Zero Trust to the Mobile Domain

For CIOs and CISOs, the goal is to decouple operational resilience from security exposure. The critical challenge is how to maintain uninterrupted access to high-privilege management interfaces during outages (the operational necessity) without extending routable network segments and expanding the attack surface (the security risk). Solving this requires an architectural shift: moving the Zero Trust enforcement point from the corporate edge to the cellular connectivity layer itself.

Zscaler Cellular achieves this shift by integrating the Zero Trust Exchange directly into the mobile network environment. Rather than relying on fragile perimeter assumptions, backhauls, or VPNs, Zscaler ensures that all SIM traffic regardless of geography, carrier, or device type passes through the cloud-native Zero Trust Exchange for inline inspection and unified policy enforcement. This approach transforms OOB access from an ungoverned “exception path” into a securely managed, auditable service.

Zscaler Cellular is built upon three foundational pillars designed to govern the highest-privilege access paths in the most distributed environments

Resilience Across the Global Cloud	Inline Policy and Complete Control (Zero Touch)	Microsegmentation by Default (Island of One)
OOB is intrinsically linked to disaster recovery and operational continuity, often being required during network failures. Zscaler Cellular is designed for maximum resilience by leveraging the Zscaler Zero Trust Exchange's global footprint, utilizing a minimum of two mobile networks across its 185 countries of operation to ensure continued service availability and security enforcement even during critical times.	This pillar moves OOB access from a security blind spot to a fully governed capability. All cellular-connected management endpoint traffic is controlled, protected, and governed inline via the Zero Trust Exchange. • Provides policy-based access controls and threat protection. • Delivers centralized logging and visibility into connection attempts. • Ensures consistent enforcement across heterogeneous environments without dependence on site-specific security stack	The primary consequence of OOB compromise is facilitating lateral movement and broad system control. Zscaler Cellular eliminates this risk by transforming each cellular-connected OOB endpoint into an isolated microsegment. This Zero Trust architecture delivers: • **Zero Attack Surface:** Management devices are concealed and undetectable tounauthorizedparties. • **Least-Privilege Access:** Only explicitly permitted and authorized communications are allowed through the Zero Trust Exchange. • **Blast Radius Reduction:** A compromised endpoint cannot pivot to other management devices or internal systems, significantly limiting the scope of any potential breach

By adopting this architectural shift, enterprises can gain resilient OOB access without expanding the network perimeter. This results in a reduced attack surface, unified policy governance across multi-country deployments, enhanced visibility for forensic investigation, and simplified, controlled third-party access for MSPs and vendors. Conclusion: Making OOB Secure, Auditable, and Operationally Scalable.

OOB management is indispensable for operational resilience, but traditional methods relying on VPNs and network backhauls force a security compromise. These high-privilege access paths bypass core Zero Trust controls and expand the routable attack surface across dispersed, heterogeneous environments.

The strategic imperative for CIOs and CISOs is clear: move OOB from a vulnerable exception to a natively secure, governed service. Zscaler Cellular achieves this architectural shift by extending the Zero Trust Exchange directly to the cellular domain, delivering inline policy enforcement and unified governance, and eliminating perimeter-based complexity. By providing "island of one" microsegmentation for every cellular-connected endpoint, Zscaler Cellular ensures OOB access is simple, auditable, and inherently secure, guaranteeing operational reach without compromising security posture.

Executive Outcomes: Resilience, Governance, and Cost Optimization

The adoption of a Cellular Zero Trust architecture for OOB management transitions OOB from an operational liability to a strategic asset. By fundamentally changing the way high-privilege access is provisioned and governed, Zscaler Cellular delivers clear security, operational, and financial outcomes:

Minimized Attack Surface and Reduced Breach Risk:

Legacy models extend the routable enterprise network to the cellular edge via APNs or VPNs, significantly expanding the attack surface. Zscaler Cellular replaces this broad network access with least-privilege, policy-defined connectivity, minimizing the likelihood that OOB becomes an attacker's expedient route to complete control and thereby reducing the blast radiusof any compromise

Operational Resilience Without Network Extension

The core function of OOB is preserving remote recovery capabilities during in-band failures is maintained without the architectural compromise of extending routable enterprise networks outward through VPNs or site-to-site constructs. This means high operational uptime is achieved without the corresponding increase in network exposure.

Unified, Simplified Global Governance

Managing security policy across multi-country deployments often requires complex, bespoke configurations for each carrier or region, leading to inconsistent operational practices. The Zscaler Zero Trust Exchange standardizes enforcement across all cellular connectivity globally, eliminating the complexity and cost associated with heterogeneous security designs.

Enhanced Visibility for Audit and Forensics

Security teams gain centralized, actionable insight into all connections to OOB endpoints, including their origin, policy compliance, and authorization status. This capability is critical for supporting compliance audits, real-time monitoring, incident response, and forensic investigation, transforming a traditional "blind spot" into a fully auditable service.

Controlled and Simplified Third-Party Access

Third-party vendors and Managed Service Providers (MSPs) often require deep access to OOB systems for troubleshooting and maintenance. Zscaler Cellular simplifies this process by providing controlled and auditable access that is strictly limited to the necessary management services and endpoints, preventing the unnecessary exposure of the entire remote environment.

The Strategic Imperative: Governing the Operational Lifeline with Zscaler

OOB and Lights-Out Management are indispensable for operational resilience, yet their traditional reliance on VPNs and network backhauls forces a security compromise. These high-privilege access paths bypass core Zero Trust controls and expand the routable attack surface across dispersed, heterogeneous environments.

The strategic imperative for CIOs and CISOs is clear: move OOB from a vulnerable exception to a natively secure, governed service. Zscaler Cellular achieves this architectural shift by extending the Zero Trust Exchange directly to the cellular domain. This delivers inline policy enforcement and unified governance, eliminating perimeter-based complexity. By providing “island of one” microsegmentation for every cellular-connected endpoint, Zscaler Cellular ensures OOB access is simple, auditable, and inherently secure, guaranteeing operational reach without compromising security posture.

Next Steps

To learn more about how Zscaler Cellular can secure and enable yourOut-of-band / Lights-Out Management infrastructure and for a personalized demonstration, contact a Zscaler expert today. Visit the Zscaler Cellular website or request a demo to begin your journey to a more secure and resilient support and operational system.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world’s largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Experience your world, secured.™