**Zenarmor SASE Messaging At-A-Glance Details**

### 

#### **Market Context**

The SASE market is undergoing rapid growth, driven by increasing demands for secure, scalable, and flexible access to cloud applications and distributed workforces.

* **Market Size & Growth**:  
  According to Gartner, the global SASE market is projected to exceed **$25 billion by 2027**, growing at a **compound annual growth rate (CAGR) of over 20%** from 2023.  
  Mid-market adoption is accelerating as solutions become more MSP-friendly, integrated, and cost-effective.
* **Enterprise vs. Mid-Market Dynamics**:
  + **Enterprises** typically adopt SASE to consolidate fragmented security stacks, enforce consistent policies across regions, and enable Zero Trust at scale with built-in privacy, security, and BYOE (Bring Your Own Edge)
  + **Mid-market** organizations are motivated by ease of deployment, vendor consolidation, limited in-house security staff, and rising ransomware threats.

### **Key Business Drivers**

#### 1. Hybrid Work and Cloud-First Strategies

* **Enterprise**: 80% of enterprises are implementing hybrid work strategies (McKinsey, 2024). SASE enables secure, identity-based access regardless of location or device.
* **Mid-market**: 60% of mid-sized companies accelerated their move to cloud apps post-pandemic (IDC, 2023), but lacked the infrastructure to secure them properly in addition to seeing an increase in hybrid/mobile workforce

#### 2. Lack of In-House Security Expertise (Especially in Mid-Market)

* **Mid-market**: Over **90% of mid-sized companies** lack a dedicated security team (CyberEdge, 2024). They need “plug-and-secure” solutions that are easy to deploy and manage.
* **Enterprise**: While they have SecOps teams, complexity across multiple point products leads to inefficiency and blind spots.

#### 3. Vendor and Architecture Consolidation

* SASE reduces operational overhead by combining NGFW, SWG, ZTNA, and CASB in one stack.
* **Enterprises** seek to replace fragmented legacy appliances and reduce tech sprawl.
* **Mid-market** wants fewer vendors, bundled solutions, and endpoint-first approaches that don’t require expensive appliances or PoPs.

#### 4. Compliance and Risk Management

* Regulatory frameworks like **HIPAA, PCI-DSS, and GDPR** require secure access and data protection at all times.Regulatory mandates like **HIPAA, PCI-DSS, and GDPR** demand secure, always-on data protection yet meeting these requirements becomes significantly harder with the rise of remote and distributed teams
* SASE supports consistent policy enforcement, logging, and threat prevention across users and devices.

#### 5. Real-Time Threat Protection and Zero Trust Adoption

* Zero Trust Network Access (ZTNA) is now a baseline expectation.
* **66% of organizations** say Zero Trust is a top priority for their cybersecurity strategy in the next 12 months (ESG, 2024).

**Operational Reality:**Remote, branch, and roaming users often operate from variable networks (home Wi-Fi, LTE, co-working). Legacy SASE and VPN models introduce latency, authentication friction, and PoP backhaul, all of which can drive users to bypass enforced paths. This increases risk exposure exponentially.

**ARCHITECTURAL DIFFERENTIATION, WHY ZENARMOR EXISTS**

Most legacy SASE solutions including Fortinet, Palo Alto Networks, and Zscaler are built on multi-pass, PoP-dependent architectures that route user traffic through enforcement nodes before policy is applied, adding not only latency complexity, user friction, and operational overhead but also significant cost. Since these vendors charge for the traffic routed through their PoPs, organizations end up paying twice for their internet access once to their ISP and again to the SASE provider.

When performance friction appears, users disconnect or disable secure tunnels even temporarily. The moment this happens, risk does not simply return, it compounds.

* Traffic reverts to direct SaaS or internal app access without inspection
* Session logs lose continuity
* Shadow access paths appear outside IT visibility
* Attackers exploit these windows for lateral movement and credential misuse

**Exponential Risk Curve**: **Legacy SASE exposure**   
With vendor PoP/agent-heavy SASE (Fortinet, Palo Alto, Zscaler), the exposure grows exponentially once users bypass enforcement: every minute outside inspection increases probability of compromise. Zenarmor’s architecture is explicitly **designed to remove the user incentive to bypass, thereby collapsing the exposure curve.**

**Zenarmor’s Architectural Response:**

* **Single-App, Single-Stack**: All enforcement runs in a unified engine, applied at endpoint, edge, or cloud.
* **No PoP dependency**: Inspection occurs at source; no detours.
* **Sub-second performance under full inspection**: Users don’t feel the latency that drives bypass.
* **Uniform policy enforcement** across all network contexts, without relying on perfect user behavior.

**Key tagline options:**

* THE FIRST AND ONLY SINGLE-APP, SINGLE-STACK SASE
* PLUG. SASE. EVERYWHERE.
* ONE. APP. SASE.

**Primary category-shaping tagline (anchors analyst briefings, web hero, decks:**

**“The First and Only Single-App, Single-Stack SASE”**

**For Analyst briefings:**

**“The First and Only Single-Pass, Single-App SASE”**

**Punchy campaign/ads tagline**

**Plug. Secure. Everywhere.**

“PLUG. SASE. EVERYWHERE.” works because:

* PLUG: speaks to Zenarmor’s instant activation, “plug-and-secure,” frictionless onboarding
* SASE: anchors you directly in the category (analysts, buyers, competitors immediately know the space).
* EVERYWHERE: captures distributed workforce, zero-PoP omnipresent security

**ONE. APP. SASE.**

*(Spotlights “single-app, single-stack” — the architecture that no competitor can claim.)*

**Hero Banner:** *PLUG. SASE. EVERYWHERE.  
 The first and only single-app, single-stack SASE. Zero PoPs. Infinite reach.*

**Booth / Events:** *PLUG. SASE. EVERYWHERE.  
 Instant Zero Trust, no complexity*

**Hero Banners:**

1. **PLUG. SASE. EVERYWHERE.**

**Subheadline:** The first and only **single-app, single-stack SASE**. Instant deployment, and omnipresent security that just works.

OR

* The first and only **single-app, single-stack SASE**. Zero PoPs. Infinite reach. No backhaul. No bypass. No exposure window.

**CTA:** [ Get Started ] [ Book a Demo ]

**2. ONE. APP. SASE.**

**Subheadline:** Simplify security with the **Industry’s** **only single-app, single-stack SASE**. Plug in anywhere, protect everywhere, scale without complexity.

OR

**Subheadline:** Simplify security with the **Industry’s** **only single-app, single-stack SASE**. Secure everywhere, fast enough that users never turn it off

**CTA:** [ Start Free Trial ] [ Talk to Sales ]

**3. PLUG. SECURE. SCALE**

**Other headline:**

* “Secure remote teams without forcing the slow tunnel.”
* “Keep protection on, even when users roam.”

**Zenarmor SASE Solution**

| **25 Words** | Zenarmor SASE is the industry’s first single-app, single-stack architecture delivering native Zero Trust protection across endpoints, edge, and cloud, no PoPs, no complexity.  Zenarmor delivers a single-app, single-stack SASE architecture with native enforcement on endpoint, edge, and cloud, enabling Zero Trust security without PoPs, complexity, or vendor sprawl.  Zenarmor delivers a single-app, single-stack SASE architecture with native endpoint, cloud, and edge inspection, combining Zero Trust access with deep, real-time security and threat protection.  Zenarmor enforces Zero Trust directly at the source, eliminating PoP routing and VPN bypass risks through one unified stack across endpoint, edge, and cloud. |
| --- | --- |
| **50 Words** | Zenarmor SASE redefines secure access and network security with the industry's only single-app, single-stack architecture. Built for the perimeter-less enterprise, Zenarmor delivers native Zero Trust protection at the endpoint, edge, or cloud, without relying on PoPs. Its Plug & Secure deployment enables omnipresent security in minutes, not weeks.  Zenarmor’s single-app, single-stack SASE architecture secures users, apps, and data across any environment, without relying on PoPs or legacy appliances. With native enforcement on endpoints, cloud, and edge, it delivers Zero Trust access, deep visibility, and real-time threat protection. Designed for fast deployment, operational efficiency, and scalable protection anywhere.  Zenarmor’s single-app, single-stack SASE architecture secures users, devices, and data across any environment. ***It delivers Zero Trust access and in-depth security*** with native inspection at the endpoint, edge, and cloud. Eliminate PoP dependence and legacy appliances with scalable protection, unified policy control, and real-time threat prevention in one lightweight stack. |
| **100 words** | Zenarmor SASE is the industry’s first and only single-app, single-stack SASE architecture, revolutionizing secure access and deep network security for today’s distributed enterprise and mid-market organizations. All networking and security functions are processed through a unified engine, natively on the endpoint, at the edge, or in the cloud, without reliance on PoPs. Zenarmor’s Plug & Secure architecture enables rapid deployment and consistent Zero Trust protection for users, devices, and workloads anywhere. With its privacy-conscious, MSP-ready design and zero trade-offs in performance, control, or complexity, Zenarmor simplifies SASE while delivering enterprise-grade inspection, policy control, and threat prevention from a single, unified solution.  Zenarmor offers an industry-first single-app, single-stack SASE architecture that secures users, devices, and workloads across endpoints, cloud, and edge, without the latency, cost, or complexity of PoP-based models. By unifying Zero Trust Network Access, threat inspection, and access control into one lightweight stack, Zenarmor enables consistent policy enforcement and real-time protection, wherever users connect. With flexible deployment options and native enforcement capabilities, it supports organizations of all sizes, from lean IT teams to global enterprises, seeking to simplify operations, reduce tool sprawl, and secure a distributed workforce. Zenarmor makes it possible to deploy secure access in minutes without compromising performance, privacy, or scalability.  Zenarmor combines Zero Trust access and in-depth security in a single-app, single-stack SASE architecture. With native inspection running directly on the endpoint, at the edge, and in the cloud, Zenarmor eliminates the need for PoP backhauling and multiple point products. The result is stronger security, faster performance, and lower complexity. Threat prevention, access control, content filtering, and traffic inspection are delivered through a unified engine—simplifying operations while strengthening protection. Whether securing remote users, cloud workloads, or distributed environments, Zenarmor enables consistent policy control and real-time visibility. Deploy in minutes and scale with confidence, without compromising on performance, privacy, or depth of defense. |

**Extra 25/50/100 word messaging based on our key differentiator - hybrid workforce, enforcing security where it is needed, even when user turns off VPN:**

**25 words:**

1. **Zero Trust That Follows the User, Not the Tunnel**Zenarmor stops malicious links leading to phishing, ransomware, or similar user-triggered attacks by enforcing Zero Trust locally even when VPN is off.
2. **Hybrid Work Expands Attack Surface, Zenarmor Collapses It**Hybrid users disconnect VPN, creating exposure. Zenarmor’s single-stack inspection runs on-device, blocking malicious links and similar attacks before PoP routing.
3. **Eliminates Off-VPN Exposure Windows**When users click malicious links or disable VPN, gaps appear. Zenarmor inspects at source, preventing phishing, ransomware, and similar user-triggered attacks instantly.

**50 words:**

1. **Exponential Attack Surface, Radically Reduced**Remote workers often disable VPN and still click into malicious links leading to phishing, ransomware, or similar user-triggered attacks. Zenarmor enforces Zero Trust directly at the endpoint through a single stack, blocking threats before traffic reaches PoPs or cloud services and eliminating exposure windows caused by backhaul-dependent SASE.
2. **Hybrid Work Expands Attack Surface, Zenarmor Collapses It**Most SASE platforms only inspect traffic routed to PoPs. But when users disconnect VPN or engage with malicious links leading to phishing, ransomware, or similar attacks, protection lapses. Zenarmor applies inspection locally on-device, cutting off threats and lateral movement before exposure occurs, reducing risk without adding complexity.
3. **Attack Surface Expands with Every Click, Zenarmor Stops It**Security breaks the moment VPN is off or users click malicious links tied to phishing, ransomware, or similar user-triggered attacks. Zenarmor’s single-app, single-stack architecture inspects traffic at the source, on the endpoint. eliminating PoP dependency, shrinking attack surface, and delivering consistent Zero Trust protection wherever users connect.

**100 words:**

1. **Behavioral + Architectural Risk Blocked at Source**In hybrid work environments, exposure doesn’t just come from architecture, it starts with user behavior. Employees disconnect VPN for performance and still click malicious links leading to phishing, ransomware, or similar user-triggered attacks. Zenarmor eliminates this risk by enforcing Zero Trust directly at the endpoint via a single-app, single-stack engine. By inspecting traffic before it leaves the device, without waiting for PoP routing or cloud inspection, Zenarmor blocks threats instantly, preventing lateral movement and detonation. This approach drastically reduces attack surface while simplifying operations, giving organizations real prevention, not conditional protection tied to network path.
2. **Exponential Attack Surface, Radically Reduced**

Ransomware and phishing attacks don’t wait for tunnels or PoP alignment, they start the moment a malicious link is clicked. When users disable VPN, traditional SASE stacks leave a gap before inspection. Zenarmor removes that gap by running inspection, Zero Trust enforcement, and threat control directly on the endpoint within a unified single stack. This ensures every session is protected even off-VPN, stopping phishing, ransomware, and similar user-triggered attacks before exposure escalates. Designed for distributed teams and lean IT operations, Zenarmor delivers enterprise-grade protection without reliance on PoPs, multi-vendor stitching, or backhaul logic.

1. **Hybrid Work Expands Attack Surface, Zenarmor Collapses it**Every major breach starts with a moment, VPN is off, a malicious link is clicked, and inspection hasn't started yet. Traditional SASE tools only protect what they can route, leaving user-triggered attacks like phishing and ransomware unchecked until traffic reaches a PoP. Zenarmor changes that by enforcing Zero Trust and full inspection directly on the endpoint using a single-app, single-stack architecture. This eliminates exposure windows created by routing dependencies, shrinks attack surface instantly, and ensures real-time threat prevention regardless of connection state. The result: stronger protection with zero complexity and instant deployment anywhere.

***Zenarmor SASE is the Industry’s first and only single-app, single-stack SASE solution.***

***Zenarmor is redefining secure access and network security for the modern, perimeter‑less enterprise and mid-market organizations. All networking and security functions are processed in a single pass through a unified engine within a single application.***

|  | **Messaging Pillars** | **Messages** |
| --- | --- | --- |
| **1.** | **Zenarmor SASE: Built on a single-app, single-stack SASE architecture**  **OR Zenarmor SASE: Redefining SASE security with a single-app, single-stack architecture** | **Zenarmor SASE is revolutionizing Internet security and network access with a unified, single-app, single-stack SASE architecture, redefining how organizations protect their data, apps, users, and services, offering unparalleled efficiency, simplified management, and robust security.**  **Product/Technical Notes:**   * **Hardware and platform agnostic, capable of being deployed on most x86 and ARM64 hardware supporting popular platforms like Windows, macOS, Linux, and BSD.** * **A DIY SASE architecture without the need to rely on a third-party vendor's cloud to deliver the service, essentially keeping all security and inspection services under your control and within your network borders at all times, with no shared infrastructure.** * **The industry’s first SASE solution, where the entire SASE stack has been bundled into a single, portable, and lightweight software package capable of running on endpoints, gateways, and in the cloud.** |
| **2.** | **Zenarmor SASE: Zero Trust natively enforced on every device**  **OR**  **Zenarmor SASE: Zero Touch. Zero Trust. Zero Compromise**  **OR**  **Zenarmor SASE: Endpoint-First Security. MSP-Ready Simplicity**  **OR**  **Zenarmor SASE: Native Zero Trust for a Distributed World** | **Zenarmor delivers Zero Trust security natively on any device through an endpoint-first SASE architecture purpose-built for distributed teams. Plug & Secure is Zenarmor’s signature deployment architecture, enabling instant rollout of SSE and SASE capabilities directly at the endpoint. Combined with a privacy-conscious, MSP-friendly design, Zenarmor ensures consistent, context-aware protection wherever users work, without the complexity of traditional solutions.**  **Product/Technical Notes:**   * **Context-awareness based on user, group, location, and device security posture (coming soon)** * **Multi-tenant, RBAC, and MSP/Partner-specific dashboards to support easy onboarding and management of clients.** |
| **3.** | ***Zenarmor SASE: Shift-Left Network Security, Endpoint-First Protection Anywhere*** | **Zenarmor shifts network security ‘left’ by enforcing Zero Trust policies directly on endpoints, stopping threats before they ever enter the network. This proactive approach delivers instant, location-agnostic protection without relying on centralized inspection points or vendor-controlled infrastructure.** |
| **4.** | **Zenarmor SASE: Bring your own EDGE- Security that lives where your users live**  **OR**  **Zenarmor SASE: Omnipresent Security. Zero Compromise**  **OR**  **Zenarmor SASE: Built for the Distributed Enterprises**  **OR**  **Zenarmor SASE: Inspection at the Edge, Endpoint, or Cloud, Managed From One Console** | **Zenarmor’s Plug & Secure Anywhere architecture brings enterprise-grade access and inspection natively to the endpoint, edge, or cloud, enabling omnipresent protection that adapts to your environment, scales with your business, and simplifies security without trade-offs.**  **Zenarmor empowers organizations to turn every endpoint into a self-contained SASE enforcement point, delivering Zero Trust, secure access, and traffic inspection exactly where it matters: on the device.**  **No vendor PoPs, no appliance sprawl, no middle-mile latency. Just instant, everywhere security.** |
| **5.** | ***Zenarmor SASE: Security at the Speed of Agility*** **OR**  ***Zenarmor SASE: Cloud Ready Without Limits*** | **Zenarmor secures any cloud, any workload instantly. Zero-touch deployment, no vendor lock-in, and protection at the speed of your business**  **OR**  **Any cloud. Any workload. Any time. Zenarmor delivers instant, zero-touch security with no limits, no delays, and no vendor lock-in**  **OR**  **Deploy security in seconds, any cloud, any workload, anywhere. With Zenarmor, there is no waiting, no lock-in, just instant protection**  **Product/Technical Notes:**   * **No need to expose private clouds or VPCs to the internet, Zenarmor’s ZTPA allows for direct and secure private access without the need to open any firewall ports, keeping these resources invisible to outside threats.** * **See the above pillars for additional/supplementary overlapping talking points** |
| **6.** | **Zenarmor SASE: Zero POP Dependency** | **Zenarmor SASE eliminates the need for cloud PoPs entirely. With zero PoP dependency, Zenarmor brings inspection and policy enforcement directly to the edge, cloud, or endpoint through its Plug & Secure Anywhere architecture. This fully distributed model removes the performance, privacy, and control trade-offs of traditional SASE, delivering faster, safer, and simpler security without backhauling or bottlenecks.**  **Product/Technical Notes:**   * **No more latency, as inspection can happen on the endpoint directly.** * **Immune to DC or PoP outages** * **No shared infrastructure with other clients** * **No IP blacklisting issues often related to shared infrastructure** |
| **7.** | **Zenarmor SASE: Deployed in minutes** | **Zenarmor SASE removes the friction from SASE deployments. With Zenarmor Plug & Secure Deployment, organizations can protect branch offices, remote teams, cloud workloads, and even legacy or IoT systems in minutes, not weeks. Whether integrating with existing infrastructure or running standalone, Zenarmor’s endpoint-first architecture delivers enterprise-grade SASE capabilities without the need for tunnels, cloud PoPs, or complex provisioning, making it ideal for fast-moving, resource-constrained teams.**  **Product/Technical Notes:**   * **No integration or interoperability friction often faced when adopting cloud-only SASE solutions, mainly caused by these companies acquiring this functionality, which was never designed to work together. Zenarmor, on the other hand, by design, is fully integrated from conception.** * **See the above pillars for additional/supplementary overlapping talking points** |

### **Messaging Pillars for Mid-Market At-A-Glance**

### 

### **Mid-Market Buyer Realities**

* 90% of mid-market organizations lack dedicated security teams.
* IT teams are stretched thin managing remote workers, legacy systems, and cloud transitions.
* Complex security stacks, backhauling, and multi-vendor deployments are costly and unmanageable.
* Mid-market buyers need rapid deployment, lean operations, and consistent protection—without sacrificing performance or control.
* Legacy SASE creates performance tradeoffs, those tradeoffs lead to bypass and exponential exposure.

### **Key Message:**

***Zenarmor delivers enterprise-grade SASE capabilities purpose-built for the mid-market, combining secure access, deep threat protection, and operational simplicity in a single-app, single-stack architecture. Unlike traditional solutions, Zenarmor runs natively on the endpoint, at the edge, or in the cloud, with no PoPs, no appliances, and no user-driven exposure windows.***

|  | **Messaging Pillars** | **Messages** |
| --- | --- | --- |
| **#1: Architecture** | Zenarmor SASE: Single-App, Single-Stack Architecture | Mid-market teams can’t afford complex, fragmented stacks. Zenarmor simplifies security by delivering networking and security functions through a single-app, single-stack engine, reducing overhead, risk, and complexity. |
| **#2: Deployment Simplicity** | Zenarmor SASE: Deploy in Minutes | Unlike traditional vendors that require tunnels, PoPs, or appliances, Zenarmor uses Plug & Secure Deployment to go live in minutes, protecting remote users, branch offices, and cloud workloads without heavy IT lift. |
| **#3: Endpoint-First Protection** | Zenarmor SASE: Zero Trust, Natively Delivered | Zenarmor brings security directly to every device with endpoint-native Zero Trust controls, enabling policy enforcement and threat prevention even without network backhaul or centralized routing. |
| **#4: PoP-Free Performance** | Zenarmor SASE: Zero POP Dependency | Mid-market buyers don’t need the latency and cost of PoP-based architectures. Zenarmor’s distributed design eliminates PoPs, ensuring faster protection and full control across all environments. |
| **#5: MSP-Ready Flexibility** | Zenarmor SASE: Built for MSP Delivery | With multi-tenant support, streamlined management, and fast onboarding, Zenarmor is ideal for MSPs serving the mid-market. Whether white-labeled or managed, partners can deliver robust SASE without legacy baggage. |

### 

## **Zenarmor SASE – Mid-Market Use-Case based Messaging**

## **Key Message:**

***Zenarmor SASE is Industry’s first and only single-app, single-stack SASE solution.***

***Zenarmor is redefining secure access and network security for the modern, perimeter‑less enterprise and mid-market organizations. All networking and security functions are processed in a single pass through a unified engine within a single application.***

***Zenarmor delivers enterprise-grade SASE capabilities purpose-built for the mid-market, combining secure access, deep threat protection, and operational simplicity in a single-pass, single-app architecture. Unlike traditional solutions, Zenarmor runs natively on the endpoint, at the edge, or in the cloud, with no PoPs, no appliances, and no user-driven exposure windows.***

***Zenarmor SASE simplifies and strengthens security for mid-market organizations by delivering the industry’s only single-pass, single-app SASE architecture with native enforcement at the endpoint, edge, and cloud, no PoPs, no vendor sprawl, no complex appliances. Whether protecting customer data, enabling third-party access, or replacing legacy firewalls and VPNs, Zenarmor offers enterprise-grade security that is deployed in minutes, not months.***

|  | **Messaging Pillars** | **Messages** |
| --- | --- | --- |
| **1.** | **Zenarmor SASE: Security that Grows with Your Mid-Market Business**  **OR**  **Zenarmor SASE: Unified Security for Distributed Teams and Systems**  **OR**  **Zenarmor SASE: Simple, Scalable Security for Distributed Mid-Market Teams** | **Zenarmor SASE consolidates fragmented tools into a unified SASE platform, designed for lean teams and fast-growing organizations. It protects users, workloads, and data across all environments, without relying on complex infrastructure or costly integrations** |
| **2.** | **Zenarmor SASE: Zero Trust Enforcement at the Endpoint, Cloud, or Edge**  **OR**  **Zenarmor SASE: Zero Trust Without POPs or Proxies** | **Zenarmor SASE delivers native Zero Trust enforcement without the complexity of cloud backhauling or multi-vendor orchestration. Policies are applied at the point of access, on the endpoint, edge, or cloud, ensuring secure connections from any user, location, or device** |
| **3.** | **Zenarmor SASE: Compliance-Ready by Design** | **Zenarmor SASE helps mid-market organizations meet compliance mandates without hiring a full-time security team. Built-in data protection, auditing, and visibility features make it easy to stay ahead of industry standards like HIPAA, PCI-DSS, ISO 27001, and SOC 2** |
| **4.** | **Zenarmor SASE: Deploys in Minutes, Scales for Growth** | **Zenarmor SASE Plug & Secure architecture allows you to deploy full-stack SASE in minutes, scale as needed, and secure every user, wherever they work. Perfect for fast-moving companies with lean IT or rapid expansion goals** |

**Messaging Pillar #1:**

**Zenarmor SASE: Simplified Security for Fragmented Environments**

Message:

***Zenarmor SASE consolidates fragmented tools into a unified SASE platform, designed for lean teams and fast-growing organizations. It protects users, workloads, and data across all environments, without relying on complex infrastructure or costly integrations***

### **Mid-Market Use Cases:**

* Replace legacy firewalls and VPNs with lightweight, single app single stack solution
* Secure branch offices and remote sites without deploying hardware
* Centralize policy control across M&A integrations
* Enable secure developer access to internal APIs and backend services
* Replace legacy VPNs and reduce bypass-driven blind spots
* Secure telehealth and remote clinicians without forcing slow tunnels
* Protect third-party contractors and partner access without extending PoP risk

### **Benefits:**

* Reduce tool sprawl with unified security
* Gain visibility and control across hybrid and remote environments
* Accelerate IT operations with easy, plug-and-secure deployment
* Eliminate PoP reliance and appliance provisioning

## 

## **Messaging Pillar #2:**

## **Zenarmor SASE: Zero Trust Access, Built for the Real World**

### Message:

***Zenarmor SASE delivers native Zero Trust enforcement without the complexity of cloud backhauling or multi-vendor orchestration. Policies are applied at the point of access, on the endpoint, edge, or cloud, ensuring secure connections from any user, location, or device***

### **Mid-Market Use Cases:**

* Provide secure access to cloud apps like Salesforce, Guidewire, Jira
* Control partner, broker, and contractor access to customer portals or data lakes
* Enforce posture-based policies for remote developer access
* Mitigate insider threats and unauthorized access to source code or infrastructure

### **Benefits:**

* Instant real-time policy enforcement without latency or backhauling
* Eliminate risk of unauthorized or lateral access
* Consistent Zero Trust security across hybrid teams and contractors
* No dependency on SD-WAN or third-party access brokers

## **Messaging Pillar #3:**

## **Zenarmor SASE: Compliance-Ready by Design**

### Message:

***Zenarmor SASE helps mid-market organizations meet compliance mandates without hiring a full-time security team. Built-in data protection, auditing, and visibility features make it easy to stay ahead of industry standards like HIPAA, PCI-DSS, ISO 27001, and SOC 2***

### **Mid-Market Use Cases:**

* Secure transfer of PHI across telehealth and clinical systems
* Enforce access controls and DLP for PII in insurance/claims workflows
* Simplify audit readiness for fintech APIs, customer data, or shared infrastructure
* Maintain compliance during and after M&A events

### **Benefits:**

* Meet multiple regulatory standards from one unified platform
* Built-in logging, posture checks, and access auditing
* Avoid fines or breaches without additional compliance software
* Simplify vendor access reviews and third-party risk assessments

## **Messaging Pillar #4:**

## **Zenarmor SASE: Deploys in Minutes, Scales for Growth**

### Message:

***Zenarmor SASE Plug & Secure architecture allows you to deploy full-stack SASE in minutes, scale as needed, and secure every user, wherever they work. Perfect for fast-moving companies with lean IT or rapid expansion goals***

**Mid-Market Use Cases:**

* Instant onboarding of remote users and clinicians across time zones
* Secure third-party contractors or temp staff without IT bottlenecks
* Replace aging VPNs in distributed clinics or financial branches
* Protect customer-facing services with minimal downtime

### **Benefits:**

* Instant deployment, no appliance provisioning or complex routing
* Protect remote, mobile, and on-prem staff without manual effort
* Scales to new branches, cloud apps, or partners in minutes
* Ideal for fast-growth orgs, MSPs, and M&A-driven teams