### **Zenarmor SASE Mid Market Playbook**

### **1. Current Focus: Mid-Market for Zenarmor SASE**

These organizations require robust security but demand ease-of-use, fast deployment, and cost-efficiency

| **Category** | **Range/Definition** |
| --- | --- |
| Employees | 50 to 2,500 |
| Annual Revenue | $5 million to $1 billion |
| IT/Security Staff | Typically 2 to 25 |
| Geographic Footprint | Single-country (US), multi-site or light global reach |
| Security Maturity | Moderate, often with fragmented point solutions |

### 

### **2. Ideal Customer Profile (ICP)**

* Companies with distributed or hybrid workforces
* Organizations using private, cloud, SaaS, and legacy systems
* Teams lacking full-time security expertise
* Organizations with security teams with defined priorities for SASE
* Businesses consolidating point security solutions into a unified platform
* Verticals: **Healthcare, Financial Services, Insurance**, Education, Legal, Manufacturing, Retail, Tech

### 

| **Persona Category** | **Titles to Target** | **Role in Buying Process** | **Messaging Focus** |
| --- | --- | --- | --- |
| Primary Decision Makers | • CIO (Chief Information Officer)  • VP/Director of IT  • VP/Director of Infrastructure  • VP/Director of Security / Cybersecurity  • IT Security Manager / Network Security Manager  • Head of IT / Head of Security • Compliance officers • CTOs | Own security/networking strategy and budget | Strategic value, security coverage, compliance, scalability, vendor consolidation |
| Technical Influencers | • Network Admin / Engineer  • Security Engineer / Analyst  • IT Manager / SysAdmin  • Cloud Architect / Infrastructure Architect  • IT Operations Manager  • DevSecOps Lead / Engineer | Evaluate and recommend solutions | Ease of deployment, integration, endpoint/cloud support, troubleshooting simplicity |
| Budget Holders / Approvers | • CFO (Chief Financial Officer)  • COO (Chief Operating Officer)  • Procurement Director  • Head of Risk or Compliance | Approve budget and assess financial risk | Cost-efficiency, ROI, vendor reliability, reduction of risk and audit concerns |
| Strategic Influencers | • CTO (Chief Technology Officer)  • Chief Risk Officer  • Head of Digital Transformation  • Compliance Officer | Influence long-term direction and standards | Innovation, risk posture, digital transformation alignment, regulatory fit |

**ICP Statement:**

Mid-market companies (50–2,500 employees) with distributed workforces, hybrid infrastructure, and lean IT/security teams seeking an affordable, unified SASE solution to simplify their network and security operations

**Conversational ICP Statement (No Jargon:**

For mid-sized companies with remote teams and limited IT resources who just want one simple way to secure access to apps and networks, without juggling multiple tools, managing VPN headaches, or paying enterprise vendor prices

**Business-Outcome Focused ICP Statement:**

Mid-market companies (50–2,500 employees) with distributed teams and hybrid infrastructure who need an affordable, unified network access and security platform (SASE) to eliminate tool sprawl, improve performance, and reduce operational burden on lean IT teams

**Emotional Focused ICP Statement:**

Mid-market IT teams tired of juggling complex VPNs, firewalls, and cloud security tools, looking for one clean way to securely connect users and apps anywhere without the headaches, latency, or cost of traditional SASE vendors

**Another Hook:**

Hybrid and remote users frequently disable VPN due to performance, leaving a security blind spot where ransomware/phishing attacks begin **before network inspection**. Zenarmor keeps inspection always-on with no PoP/VPN dependency.

### 

### **3. Common Pain Points and Zenarmor’s Differentiator**

| **Common Pain Points** | **Zenarmor SASE Advantage** |
| --- | --- |
| Fragmented security tools | Unified SASE stack and architecture  Delayed inspection when remote users are off-tunnel |
| Limited in-house expertise | Fast and easy deployment in minutes |
| Compliance and data protection | Integrated ZTNA, SWG, CASB, DLP, and reporting |
| Legacy firewalls/VPNs | Can run natively at the edge, in the cloud, or on the endpoint  Users turn VPN off, creates invisible attack surface |
| High cost of enterprise SASE vendors | Flexible, cost-effective licensing |

### **4. Targeting Strategy**

**Segmentation Criteria:**

* Employee count: 50 – 2500
* Revenue: $5M – $1B
* Security/IT team size: Between 2 to 25 people
* Remote-friendly and cloud-friendly businesses

**Primary Focus:**

**Verticals: *Healthcare, Insurance, Financial Service*s**, Legal, Manufacturing, Retail, technology

Secondary Focus:

* MSPs, MSSPs, and VARs serving mid-market
* Regional cybersecurity resellers

**Messaging Themes:**

* "One platform single stack to replace your VPN, NGFW, SWG, CASB, and SDWAN"
* "Mid-market security with enterprise-grade protection"
* "Comprehensive SASE, minus the complexity"
* "Affordable Zero Trust for every user, anywhere"
* “VPN Off = Attack Surface +300%, Zenarmor enforces Zero Trust access without relying on VPN tunnels or PoPs.”

### **Industry Pain Points and Zenarmor Messaging**

| **Industry** | **Key Pain Points** | **Zenarmor Messaging for Pain Points** | **Sales Talking Points** |
| --- | --- | --- | --- |
| Insurance | * Legacy VPNs and firewalls * Remote agent access * Ransomware threats * Regulatory compliance burden * Limited IT headcount | * ZTNA for secure access * All-in-one SASE stack * Compliance-ready architecture * Endpoint based deployment * MSP-friendly model | * **SSE for field agents**: Replace VPN with secure, identity-aware access * **Endpoint-based architecture**: No appliance required for branch offices * **Built-in compliance mapping:** Tools to support GLBA/NAIC (Gramm-Leach-Bliley Act, National Association of Insurance Commissioners) requirements * **Threat prevention & data protection**: SWG, CASB, and DLP integrated in a single stack * Field agents often work off-tunnel — Zenarmor ensures **always-inspected connections**, even when VPN is off. |
| FinTech | * DevOps outpacing security Multi-cloud exposure- PCI * DSS and SOC 2 demands * SaaS visibility gaps * Real-time posture needs | * API-first SASE * Instant-on CASB/ZTNA * Prebuilt compliance policies * SaaS visibility * Continuous monitoring & threat detection | * **Instant-on SASE stack for developers**: Protect users, apps, and APIs in minutes * **ZTNA with fine-grained access control**: Segment access to back-end services * **Audit-ready architecture**: Logging, access reports, and DLP policies for compliance * **Dev-friendly integration**: API-driven policies that fit into CI/CD pipelines * Dev teams often work off-tunnel — Zenarmor ensures **always-inspected connections**, even when VPN is off. |
| Healthcare | * HIPAA/PHI data risk * Budget constraints- Outdated EHRs * Staff untrained in cybersecurity * Rise in phishing/ransomware | * HIPAA-aligned policies * Low-cost endpoint SSE * Data and app protection * Lean deployment * Secure telehealth & EHR (electronic health record) support | * **Plug-and-secure ZTNA for clinical apps**: Secure access to EHRs and internal tools * **HIPAA-ready data controls**: Built-in SWG, CASB, and DLP to protect PHI * **Distributed protection**: Extend SSE down to endpoints (not just edge network) * **Low total cost of ownership**: Avoid expensive appliances or complex multi-vendor vendor stacks * Clinicians often work off-tunnel — Zenarmor ensures **always-inspected connections**, even when VPN is off. |

### 

**More Hooks/Questions to Ask:**

* When VPN is off, your SSE stack is blind. How are you handling that today? Then position Zenarmor as the answer.
* Unlike legacy VPN/PoP SASE models that lose visibility the moment a remote user disconnects, Zenarmor keeps full-stack inspection active at the endpoint — closing the ransomware/phishing gap created by VPN-off scenarios
* How do you enforce security when users disconnect from VPN because of performance, do you accept that blind spot or do you have a workaround?

**Key Themes Across Insurance Industry Use Cases that Zenarmor SASE solves for:**

* *Zero Trust by default:* No more network-based assumptions of trust
* *Designed for hybrid work:* Agents, underwriters, and claims staff can work anywhere
* *Compliance and audit alignment:* Structured visibility and control help simplify audits
* *Cost-effective scale:* No branch hardware, ideal for regional insurers and franchises

**Mid-Market Insurance Industry Use Cases for Zenarmor SASE**

| **Insurance Organizations Use Cases** | **How Zenarmor SASE helps** |
| --- | --- |
| **Remote Agent Access to Claims/Underwriting Apps** | ZTNA enables secure, identity-aware access from any device/location without VPN |
| **Secure Access for Third-Party Adjusters or Contractors** | Granular policy control and time-limited access via ZTNA |
| **Cloud App Protection (e.g., Salesforce, Guidewire) The risk is exponentially elevated for**  **home/branch/remote workers rather than just from corporate office** | CASB and SWG protect against data exfiltration, misconfigurations, and shadow SaaS |
| **Ransomware Protection at Remote Sites/Offices** | DNS security, threat intelligence, and endpoint inspection without hardware |
| **Data Loss Prevention for Customer PII from remove locations** | Built-in DLP controls and reporting help meet GLBA and state-level requirements |
| **Mobile Access** | Zenarmor SSE stack (ZTNA + SWG + CASB) protects web portals and apps from unauthorized access |
| **Branch Office Security Without Appliances** | Zenarmor Endpoint-based SASE removes the need for costly NGFWs at every site |
| **Regulatory Compliance who are removed from corporate network** | Policy templates, access logs, and reporting aid audits and simplify ongoing compliance |
| **Unified Protection Across M&A Integrations** | Centrally managed policies help streamline and secure acquisitions and business units |
| **Partner and Broker Access Enablement** | Secure app segmentation with ZTNA ensures only the right parties access sensitive data. Faster speed of deployment and connection), better visibility and control |
| **Remote Access** | Eliminates VPN gap, inspections continue even when users drop tunnel due to latency |

## 

**Key Themes across FinTech Use Cases that Zenarmor SASE solves for:**

* “Developer-first” culture where speed and flexibility matter
* Security posture that keeps up with product velocity
* Protection across cloud-native and SaaS-first ecosystems
* Low overhead, high automation for scaling securely

**Mid-Market Financial Services Use Cases that Zenarmor SASE solves for:**

| **Financial Services Use Cases** | **How Zenarmor Helps** |
| --- | --- |
| **Developer Access to Back-End Services & APIs esp. remote users** | ZTNA replaces VPNs with granular access to cloud services, CI/CD tools, and databases |
| **Protecting SaaS Tools (e.g., Notion, Jira, Slack) esp. remote/hybride/mobile** | CASB ensures visibility and enforces policy on cloud tools often used in shadow IT |
| **Preventing Unauthorized Code Repo Access** | Application-layer policies restrict GitHub, Bitbucket, and internal repo access |
| **Securing Remote Workforce in Global Time Zones** | Endpoint-based SASE ensures always-on protection regardless of network or location |
| **Compliance with PCI-DSS, SOC 2, ISO 27001** | Integrated DLP, SWG, CASB, and logging help enforce controls and streamline audits |
| **Zero Trust Access to FinCore, Banking APIs, Data Lakes** | ZTNA ensures user/device verification before granting access to sensitive data systems |
| **Secure SaaS Authentication (e.g., Okta, Workday)** | Identity-aware policies prevent session hijacking or cross-user access in shared apps |
| **Mitigating Risk from Acquisitions & Shared Infrastructure** | Unified policies segment access across inherited or multi-tenant environments |
| **Real-Time Posture Enforcement During DevOps Deployments** | Lightweight agent validates user posture before granting access to prod infrastructure |
| **Protecting Customer-Facing Apps from Insider Threats** | SWG and DLP prevent data leaks or misuse from internal roles accessing user PII |
| **Controlling Access to Embedded FinTech Infrastructure (Plaid, Stripe, AWS)** | Granular access controls enforce least privilege across embedded fintech providers |
| **Developer Access** | Eliminates VPN gap, inspections continue even when users drop tunnel due to latency |

**Key Themes Across Healthcare Industry Use Cases that Zenarmor SASE solves for:**

* Compliance-Ready: HIPAA and audit-aligned by design
* Zero Trust Access: Secure, identity-aware remote access for clinicians and staff
* Lean IT Fit: Easy to deploy and manage with limited security resources
* No Hardware Needed: Endpoint-based protection across clinics and remote teams
* PHI Protection: DLP, SWG, and CASB secure cloud apps and SaaS tools
* Third-Party Access Control: Granular policies for vendors, labs, and partners
* Telehealth Security: Real-time protection for virtual care sessions
* Scalable for Growth: Flexible licensing across clinics, staff, and branches

**Mid-Market Healthcare Services Use Cases:**

| **Healthcare ServicesUse Cases** | **How Zenarmor Helps** |
| --- | --- |
| **Secure Access for Remote Clinicians and Staff** | ZTNA ensures only authorized users and trusted devices access EHRs and clinical apps |
| **Protection of PHI Across SaaS and Cloud Services** | CASB and SWG enforce DLP policies across email, file sharing, and collaboration tools |
| **HIPAA-Compliant Data Transfer & Auditing** | Built-in logging, encryption, and access policies support audit readiness |
| **Replace Aging VPNs in Distributed Clinics and Practices** | Endpoint-based ZTNA and SSE eliminate the need for complex, hardware-based VPNs |
| **Centralized Security Across Merged or Acquired Clinics** | Unified policy enforcement across decentralized networks with minimal IT overhead |
| **Telehealth Session Security** | Real-time traffic inspection and Zero Trust policies ensure secure video consultations |
| **Remote staff Security Gaps & Phishing Mitigation** | Threat protection and SWG block malicious links, domains, and browser exploits |
| **IT Staff Efficiency for Small Security Teams** | Plug-and-play deployment and centralized visibility reduce admin burden |
| **Secure Integration with Payers and External Labs** | Granular ZTNA controls access to APIs, portals, and sensitive apps for third parties |
| **elehealth Access** | Eliminates VPN gap, inspections continue even when users drop tunnel due to latency |

### **5. Packaging & Pricing Recommendations**

Product tiers:

* **Zenarmor SSE**: SWG, CASB, NGFWaaS, Deep TLS Inspection
* **Plug and Secure SSE with ZTNA as add-on option**
* **Zenarmor ZTPA** (Zero Trust Private Access)
* **Zenarmor SASE**: SSE + SDWAN functionality

Offer flexible per-user/month pricing with volume discounts and MSP options.

### 

### **6. Sales Toolkit**

* Mid-market Zenarmor SASE vertical solution briefs - Asha
* 4 short videos (1 minute each) showcasing Zenarmor SASE/SSE features, benefits, onboarding flow, reporting - Lyal, Hien
* Competitive battlecards (Zenarmor vs. Zscaler, Fortinet, Cato) - Lyal
* ROI calculator for CISOs, CTOs, CFOs and IT managers - Asha
* Compliance checklist: HIPAA, SOC 2, PCI - Asha
* Case studies (later) - Emrah

### 

### **7. KPIs and Success Metrics**

* New mid-market free trials added
* New mid-market accounts added
* MSP/channel pipeline contribution
* Customer retention and upsell rates

### 

### **8. Next Steps**

* Create mid-market campaign
* Launch mid-market campaign
* Review campaign metrics quarterly