TPx Managed SASE: Technical Deep Dive

TPx Managed Secure Access Service Edge (SASE) brings together cloud-delivered security, Zero Trust access, and modern networking into a single managed solution. We simplify Zero Trust adoption through curated, easy-to-consume Security Service Edge (SSE) bundles that integrate with your current identity systems, TPx Managed SD-WAN or integrated into an existing WAN, customers gain a complete, flexible, and future-ready SASE strategy. SASE = SD-WAN + SSE.

What is Managed SASE/SSE — and Why It Matters

Traditional VPNs, firewalls, and hub-and-spoke architectures rely on network trust and perimeter boundaries that no longer align with remote work, SaaS adoption, or distributed environments.

Managed SASE/SSE modernizes security by:

- Moving access control and threat inspection to the cloud
- Applying Zero Trust principles (verify every connection, allow only what's needed)
- Connecting users directly to applications instead of the corporate network
- Eliminating lateral movement and shrinking the attack surface
- Improving performance by removing backhauling and VPN bottlenecks

TPx manages the entire service end-to-end, providing stronger security and simpler operations without adding complexity for IT.

The Cloud Security Fabric: How It Works

At the core of TPx Managed SSE is a cloud-based security fabric that performs identity enforcement, policy evaluation, traffic inspection, and application access control — all without requiring users to connect to a corporate network.

The fabric continuously:

- **Authenticates identity** using your existing IdP
- **Validates device posture** (OS, health, compliance)
- **Applies business and security policies** in real time
- **Connects users directly to authorized applications**
- **Inspects traffic inline** for threats and data risks

Applications remain hidden and only become reachable when policy allows it, preventing lateral movement and reducing exposure.

Zero Trust Principles Used

- No implicit network trust
- Users connect to specific apps/services (not the network)
- Every session is authenticated, authorized, and inspected
- Policies follow users everywhere they work
- Security and performance improve simultaneously through direct-to-cloud access

Core Technical Components Delivered Through TPx Managed SSE

Secure Web Gateway (SWG)

A cloud-delivered security layer that inspects outbound internet and SaaS traffic in real time.

Key functions:

- Malware, ransomware, and phishing defense
- SSL inspection
- Shadow IT visibility and control
- URL filtering, content policies, and compliance enforcement
- Inline data loss protection for web-based activity

Outcome: Safe, compliant, high-performance internet and SaaS access with no hardware or backhauling.

Zero Trust Network Access (ZTNA)

Replaces VPNs by providing identity-based access to private applications — without placing users on the network.

ZTNA enables:

- Direct, encrypted connections from user → application

- Enforcement of least-privilege access based on identity + device posture
- Preventing applications from being discoverable or exposed publicly
- No network-level access; users only reach allowed app endpoints

Outcome: Fast, secure private app access without VPNs or lateral movement risk.

Cloud Firewall / DNS Security

A cloud-native alternative to traditional perimeter firewalls.

Capabilities include:

- Outbound/ingress policy control
- DNS filtering and threat protection
- Blocking command-and-control (C2) callbacks
- Application-layer filtering

Outcome: Firewall-grade protection everywhere users connect — with no appliances.

Cloud Access Security Broker (CASB)

Provides control and governance over SaaS applications.

CASB capabilities:

- Discovery of sanctioned/unsanctioned SaaS usage
- App-level data sharing controls
- API-based posture scanning for misconfigurations
- Activity monitoring and alerting

Outcome: Reduced SaaS risk, visibility into shadow IT, and better governance.

Data Loss Prevention (DLP)

Inline and API-based inspection detects and blocks unauthorized movement of sensitive data.

DLP supports:

- Structured and unstructured data detection
- Inline blocking or redaction
- SaaS file scanning and policy enforcement
- Compliance mapping (HIPAA, PCI, CJIS, etc.)

Outcome: Protected data across web, SaaS, private apps, and cloud storage.

AI/GenAI Security Controls

Visibility and enforcement over GenAI tool usage.

Provides:

- Monitoring of prompts and responses
- Detection of sensitive content being submitted or generated
- Governance over which AI tools users may access
- Inline restrictions where needed

Outcome: Safe, compliant adoption of AI tools without data exposure.

Identity Integration (IdP-Centric Security)

TPx integrates SSE directly into your existing authentication system:

- Microsoft Entra ID
- Okta

Identity and contexts become the foundation of every access decision.

Benefits:

- No change to user login experiences
- No directory migration
- Unified, consistent access policies
- Immediate alignment with Zero Trust best practice

How TPx Simplifies Adoption

Cloud security platforms are powerful but complex. TPx simplifies them with:

- Curated bundles (Secure Access, Data Governance)
- Policy design and architecture assistance
- Identity and network integration
- Continuous tuning and optimization
- Unified support and troubleshooting
- No need for internal SSE or Zero Trust expertise
- An ongoing partnership with Quarterly Business Reviews to aid adoption and scale

TPx delivers the platform as a fully managed service — customers get outcomes, not complexity.

End-to-End Managed Delivery

TPx operates the service throughout its lifecycle:

- Architecture and readiness assessments
- Identity and network integration
- Policy creation and tuning
- Change management and threat analysis
- Centralized logging and reporting
- Ongoing monitoring and incident handling
- Migration from VPNs, firewalls, and legacy technologies

Outcome: A Zero Trust security architecture that operates seamlessly without requiring customer resources, or an all at once rip-and-replace.

SSE + TPx SD-WAN = Full SASE

TPx is uniquely positioned to provide both the networking and security components of SASE.

Security (SSE)

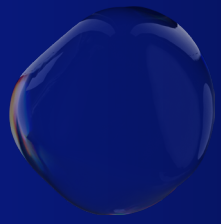
- Cloud-based Secure Web Gateway (SWG)
- Zero Trust Network Access/Private Application Access (ZTNA)
- Cloud Access Security Broker (CASB)
- Data Loss Prevention (DLP)
- Cloud Firewall
- In-line inspection

Networking (SD-WAN)

- **WAN Optimization:** Streamlines data flows and minimizes latency to improve performance for critical business apps.
- **Quality of Service (QoS):** Prioritizes bandwidth dynamically so essential applications stay smooth even under heavy load.
- **Intelligent Routing:** Selects the best available network path in real time based on application type, performance, and policy.
- **SaaS Acceleration:** Optimizes traffic to leading SaaS platforms—like Microsoft 365, Teams, and Salesforce
- **Content Delivery & Caching:** Caches frequently accessed content locally to reduce bandwidth use and speed up response times.
- **Automated Failover:** Detects link degradation or outages instantly and reroutes traffic automatically to maintain uptime.

Customers can:

1. Use TPx SD-WAN to build a unified SASE architecture, or
2. Keep their current SD-WAN and layer TPx SSE on top without disruption.



Customer Transformation

Before SSE/SASE	After TPx Managed SSE/SASE
VPN bottlenecks	Security becomes simpler and more scalable
Inconsistent security controls	All traffic is authenticated and inspected in the cloud
Backhauled traffic	Performance improves significantly
Exposed applications	Applications become invisible and protected
High lateral movement risk	Users connect directly to apps, not networks
Limited SaaS and AI visibility	Data is governed across SaaS and AI tools Security becomes simpler and more scalable

The Bottom Line

TPx Managed SSE delivers a modern security architecture built on Zero Trust principles, cloud-delivered inspection, and identity-based access; without requiring organizations to build or manage the platform themselves. Combined with TPx SD-WAN or integrated into an existing WAN, customers gain a complete, flexible, and future-ready SASE strategy.