WHITE PAPER: SARAHAI-ZERO_TRUST

A Next-Generation Zero Trust Security Framework for Enterprises & Telco-Grade Networks

Executive Summary

As organizations embrace cloud, IoT, remote work, and 5G edge computing, the traditional perimeter-based security model is no longer sufficient. **SARAHAI-ZERO_TRUST** is a next-generation **Zero Trust Security Framework** that enforces **continuous verification, dynamic access controls, and real-time anomaly detection** to secure modern distributed enterprises and telco-grade networks.

Unlike legacy **NAC (Network Access Control)** or **firewall-based** approaches, SARAHAI-ZERO_TRUST leverages **advanced AI-driven anomaly detection**, **real-time network analytics**, and **adaptive security policies** to proactively detect and mitigate security threats—**before they impact operations**.

By integrating with **SARAHAI-NIDS (Network Intrusion Detection System)** and **SARAHAI-SIEM (Security Information & Event Management)**, this solution **provides unparalleled visibility, reduces attack surfaces, and enables Zero Trust access across multi-cloud and hybrid infrastructures.**

Business Benefits of SARAHAI-ZERO_TRUST

1. Proactive Threat Detection & Response

- **Pattern-of-Life Intelligence:** Uses **Kernel Density Estimation (KDE) & Isolation Forest Machine Learning** to detect deviations from normal behavior.
- **Adaptive Anomaly Response:** If abnormal activity is detected (e.g., unauthorized lateral movement or high-volume data transfers), automated responses (like session termination or MFA escalation) are triggered.

2. Micro-Segmentation for Stronger Network Security

- **Least-Privilege Access**: Ensures that users and devices only access the necessary network segments.
- **Dynamically Adapts to Threat Intelligence**: If a device is flagged as compromised, its access is automatically restricted.

3. Seamless Integration with Multi-Cloud & On-Prem Networks

- **Supports Hybrid Workforces**: Extends Zero Trust security policies across **on-prem, cloud, and remote users.**
- **Protects Edge & IoT Deployments**: Ideal for **5G, SD-WAN, and IoT** ecosystems where security risks exist outside the traditional perimeter.

4. Reduces False Positives & Security Fatigue

- **AI-Driven Threat Detection**: Reduces alert overload by focusing on **high-risk** behaviors instead of static, rule-based alerts.
- **Adaptive Thresholding**: Continuously adjusts the anomaly threshold based on observed network behavior.

5. Simplifies Compliance & Auditability

- **Granular Audit Trails**: Logs every user and device action for compliance with **GDPR, HIPAA, PCI DSS, and CMMC**.
- **Built-In OpenDocument Spreadsheet (ODS) Reporting**: Generates compliance-ready reports with one click.

Technical Architecture: How SARAHAI-ZERO_TRUST Works

SARAHAI-ZERO_TRUST enforces **continuous verification and dynamic security policies** using **six core components**:

1. Identity & Device Authentication

- Integrates with **SSO (Single Sign-On), Multi-Factor Authentication (MFA), and Identity Providers (IdPs)** to validate users and devices.
- Supports **continuous authentication**—revalidating users based on risk-based scoring.

2. Micro-Segmentation Controllers

- Divides the network into **granular segments** (e.g., Finance, R&D, IoT devices) with independent security policies.
- Ensures that **no lateral movement** occurs between segments unless explicitly allowed.

3. Adaptive Security Layer (ASL)

- **Real-time anomaly detection** via **SARAHAI-NIDS** and **SARAHAI-SIEM**.
- **Machine Learning-powered Behavioral Analytics** to detect unauthorized access, account takeover, or advanced persistent threats (APTs).

4. Continuous Monitoring & Risk-Based Access

- Each session is continuously analyzed for **risk score fluctuations**.
- If a session is flagged as suspicious, access can be **denied, restricted, or escalated to additional verification**.

5. Distributed Enforcement Points

- **Sensors deployed across data centers, cloud workloads, SD-WAN, and IoT edge nodes** ensure that security enforcement happens **close to the data**.
- Enables **scalable** deployment across **large enterprises, telcos, and critical infrastructure**.

6. Real-Time Threat Intelligence & SIEM Integration

- Security insights are **aggregated into SARAHAI-SIEM** for **centralized visibility, compliance tracking, and policy updates**.
- Can integrate with **Splunk, Microsoft Sentinel, IBM QRadar, Cisco SecureX, or Open Threat Exchange (OTX)**.

Competitive Comparison: SARAHAI-ZERO_TRUST vs. Industry Leaders

Feature	**SARAHAI-ZERO_TRUST**	**ZScaler Zero Trust**	**Palo Alto Prisma Access**	**Cisco Zero Trust**	**Microsoft Defender for Cloud Apps**
Adaptive Anomaly Detection (KDE, ML)	✅ Yes	❌ No	❌ No	❌ No	❌ No
Pattern-of-Life Behavioral Analytics	✅ Yes	❌ No	❌ No	❌ No	✅ Yes (basic heuristics)

Feature	SARAHAI-ZERO_TRUST	ZScaler Zero Trust	Palo Alto Prisma Access	Cisco Zero Trust	Microsoft Defender for Cloud Apps
Micro-Segmentation (Dynamic Controls)	✅ Yes	✅ Yes	✅ Yes	✅ Yes	❌ No
AI-Driven Risk-Based Access	✅ Yes	✅ Yes	✅ Yes	✅ Yes	❌ No
SIEM Integration (Splunk, QRadar, etc.)	✅ Yes	✅ Yes	✅ Yes	✅ Yes	✅ Yes
Edge & IoT Security	✅ Yes (5G, SD-WAN, MEC)	❌ No	❌ No	❌ No	❌ No
Continuous Verification	✅ Yes	✅ Yes	✅ Yes	✅ Yes	✅ Yes
Hybrid Multi-Cloud Deployment	✅ Yes	✅ Yes	✅ Yes	✅ Yes	✅ Yes
OpenDocument Spreadsheet (ODS) Export	✅ Yes	❌ No	❌ No	❌ No	❌ No

---

Why SARAHAI-ZERO_TRUST Stands Out

1. **Unified Anomaly Detection & Access Control**: Unlike traditional Zero Trust solutions, SARAHAI-ZERO_TRUST actively **analyzes network traffic for threats** and adjusts security policies dynamically.
2. **Designed for Enterprise, Telco, and Edge**: Supports **on-premises, cloud, 5G edge nodes, and SD-WAN architectures**.
3. **Deep SIEM & Threat Intelligence Integration**: Unlike Microsoft or Cisco's solutions, which focus on device authentication, SARAHAI provides **real-time intrusion analysis and continuous monitoring**.
4. **Fully Extensible**: Integrates with **custom policy engines, AI-based scoring models, and industry-specific compliance workflows**.

Deployment Models

1. On-Premises Deployment

- Deploy Zero Trust **micro-segmentation controllers** inside existing data centers.
- Monitor internal traffic using **SARAHAI-NIDS sensors**.

2. Cloud-Native Deployment

- Deploy enforcement points across **AWS, Azure, Google Cloud** to secure VPC workloads.
- Secure **SaaS applications** via **Zero Trust API Gateways**.

3. Edge Computing & IoT Security

- Monitor IoT and **5G MEC (Multi-Access Edge Computing)** networks.
- **Detect and isolate compromised IoT devices** before they impact operations.

Conclusion: The Future of Zero Trust Security

SARAHAI-ZERO_TRUST is the **first truly adaptive, anomaly-driven Zero Trust solution**, delivering:

✓ **Proactive Threat Prevention** (Before Attackers Move Laterally)
✓ **Seamless, Risk-Based Authentication** (Minimizing User Friction)
✓ **Edge & IoT Security Readiness** (For Telco-Scale Deployments)
✓ **SIEM & Threat Intelligence Integration** (For Complete Security Insights)

Organizations that adopt **SARAHAI-ZERO_TRUST** gain a **future-proof** security framework designed to handle today’s sophisticated threats while simplifying operations and **ensuring compliance**.

Next Steps

To learn more, schedule a demo, or request a proof-of-concept (PoC), contact **Tensor Networks, Inc.** at:

📧 **Email**: information@tensornetworks.net

🌍 **Website:** www.tensornetworks.com

End of White Paper