KITE CYBER
info@kitecyber.com | https://www.kitecyber.com

Hyperconverged Endpoint Security: Endpoint SWG, NG ZTNA, NG DLP, Device Management

Challenges with existing solutions

Broken Security & Compliance

- **Invisible SaaS and Gen AI apps**
  What's your unapproved app usage
- **Invisible Data Activity**
  Which user devices have sensitive data
- **Invisible User Activity**
  How many unsafe links accessed

Complexity

- High risk from **siloed security** tools
- **Agent fatigue:** Device Management, VPN, SSE & Compliance
- Traffic **hair-pinning** causes poor UX

Cost

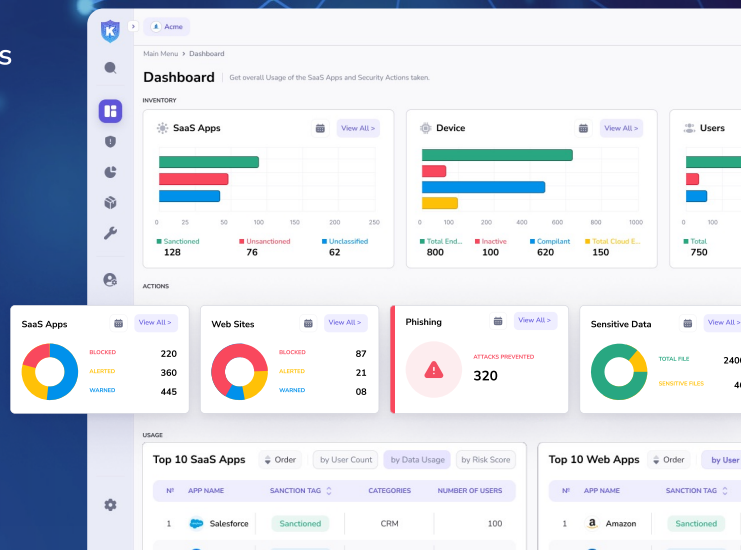
- Cloud & near edge based solutions are **expensive**
- Needs **trained experts** for deployment
- **Tradeoff** between security & cyber insurance

Kitecyber vs. Traditional SASE or SSE Solutions

Requirements	KiteCyber	SASE/SSE	Why Kitecyber?
Security & Compliance gaps			
• Invisible SaaS and Gen AI apps	✓	✗ Limited to apps in SSO	SOC 2 CC 6.2 & CC 6.3, PCI DSS A3.2.6, CSA 5, NIST 800-53 - SC-7(19), NIST 800-171-3.13.1
• Invisible Data Activity	✓	✗ Limited to reputation based filtering	FFIEC, CIS 14.7, NIST 800-171 - 3.13.1, NIST 800-53 -SC-7(19), CSA 2.1.2.3
• Invisible User Activity	✓	✗ Limited to low % of TLS traffic	SOC 2 CC 6.7, CSA 3.1.1.16, CSA 3.1.1.18, CIS 14.7, FFIEC, NIST 800-53 -SC-7(10)
Complexity	Low	High	No cloud gateway or appliance needed
Cost	Cost Effective	$$$ Expensive	Endpoint based distributed architecture. No gateway cost for customers

Use Cases

- **Compliance:** Enforce & automate compliance controls
- **Endpoint SWG:** Shadow SaaS App, Shadow AI
- **NG DLP:** Discover Sensitive Data & Manage Unauthorized Data Transfers
- **NG ZTNA:** Zero Touch private access, password less, device trust based
- **MDM:** Device Management for corporate, BYOD and contractors
- **Safe Browser:** Real time Phishing and identity theft prevention



KITE CYBER

info@kitecyber.com | https://www.kitecyber.com

Introducing Kite Cyber Hyper Converged Endpoint Security

App Shield for Shadow SaaS & AI apps

- **Discover** all SaaS Apps and supply chain API inventory
- **Monitor** user's abnormal app usage
- **Access controls** based on user posture and app category.

User Shield for Real time phishing prevention

- **Prevent** internet threats using multi-model AI inference
- **Trust score** identifies risky user behaviors
- **Visibility** into all user IP traffic activity for risk assessment

Data Shield for Sensitive Data Activity

- **Discover** sensitive data
- **Prevent** sensitive data leaks & exfiltration
- **control** sensitive data with device lock, remote wipe for lost devices

Device Shield for Device Compliance

- **Enforce** compliance controls across corporate, BYOD & Contractors
- **Access controls** to trusted website access using secure DNS
- **Prevent** unauthorized activity using Host firewall

Infra Shield Zero Trust Private Access

- **Zero Touch** private infrastructure access
- **Passwordless** with security risk based posture management
- **Privacy by Design,** deploy in Your Own Infrastructure with your Encryption keys

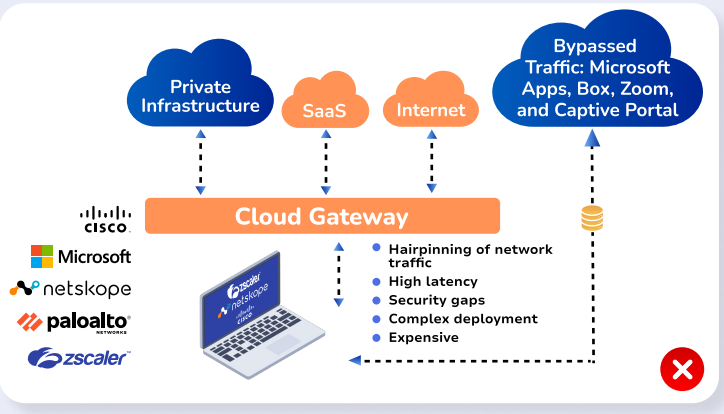
User Behavior Analytics

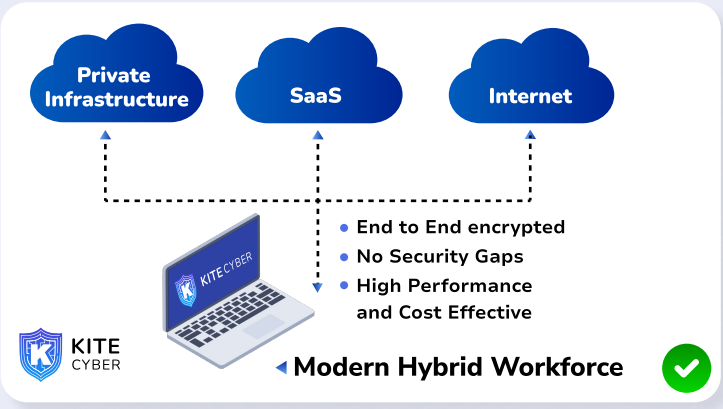
- **User behavior** profiling based on user role and activity signals
- **User segmentation** based on role, location and sensitive data access
- **Anomaly detection** based on unusual access patterns

Kitecyber vs. Existing SASE or SSE Solutions

Traditional SSE

- Security Gaps in SaaS app visibility, Phishing and sensitive data visibility
- Poor user experience due to hairpinning
- Complexity with weeks & months of deployment cycle:
- Cost of data processing in the cloud and near edge locations
- No device management





Endpoint Based SSE

- No Security Gaps
- High performance, low latency
- Deployment in minutes
- Cost effective leveraging state of art edge processing
- Hyperconverged endpoint security in SSE, Device Management, Private Access and Data Security using device trust