KITE CYBER

Endpoint-First Secure Web Gateway

Challenges: Blindspots & policy exceptions erode Zero Trust

Visibility & Blindspots

- Split tunneling & Exceptions hides traffic
- Offline or roaming users go unprotected
- Agentic/Gen AI apps evade URL filters

Evasion & Bypass Risks

- Trusted CDNs exploited for payload delivery
- Domain-based allowlisting enables bypass
- Policy exceptions erode enforcement.

Performance & Overhead

- SSL/TLS decryption adds significant latency
- Policy pushes take excessive time
- Frequent false positives frustrate users

Kitecyber Approach - Endpoint First SWG

Close Zero Trust Gaps

- Agent-based inline inspection
- Monitors SaaS, web, Gen AI
- Enforces policies offline too

Prevent Zero Day Evasions

- Inline policy enforcement agent
- Blocks CDN-based exploit attempts
- Unified SaaS and web controls

Low Operational Overhead

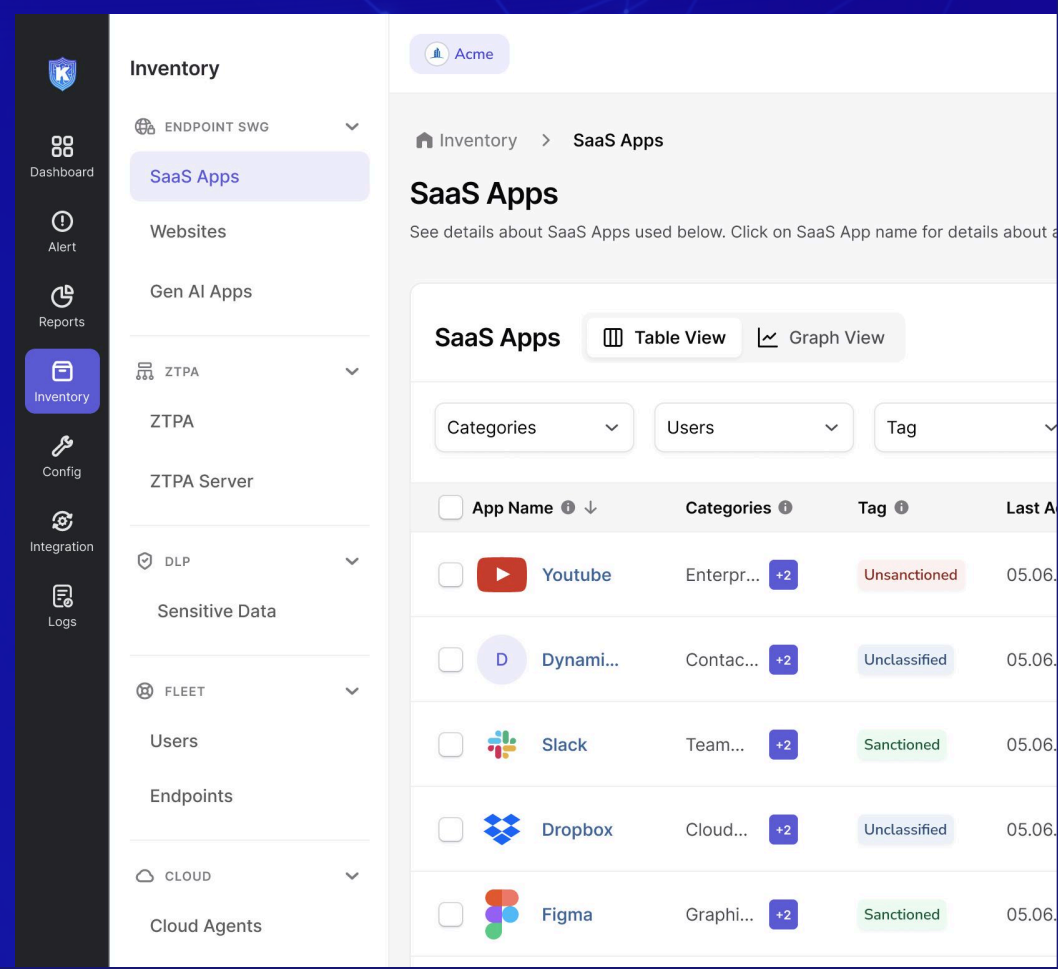
- Agent-based local policy enforcement
- No traffic hairpinning delays
- Instant policy update propagation

Use Cases

- **Anti-Ransomware Protection** from Malicious Links, Data Exfiltration and Endpoint Managed Disk Encryption & Passwords
- **Endpoint Zero Trust** with device security and compliance posture monitoring and enforcement
- **Low overhead** with seamless onboarding, unified console for modern security stack of Device Management, DLP, ZTNA and SWG
- **Audit-ready Compliance** with pre-mapped security controls, real time compliance dashboard and automated evidence collection

Next-Gen SaaS, Gen-AI & Internet Security

Visit **www.kitecyber.com** for more details!



KITE CYBER

691 S Milpitas Blvd, Ste 217, Milpitas, CA 95035
Email: info@kitecyber.com,
Website: www.kitecyber.com

Customers love us!

G2 ★★★★★ | Capterra ★★★★½ | GetApp ★★★★½ | Software Advice ★★★★½

ISO 27001 Certified

SOC 2 Type II compliant