BROADCOM

The Strategic Case for Web Traffic Inspection Beyond the Endpoint

Web traffic is everywhere—and securing it requires visibility beyond managed devices.

Key Topics

Why This Matters → SWG + EDR → The Visibility Gap → SWG Inspection Life Cycle → What's at Stake → Cloud SWG Capabilities → Business Outcomes → Bottom Line

Why This Matters

Organizations have invested heavily in endpoint security, but a growing percentage of enterprise traffic never reaches systems monitored by endpoint agents.

Cloud applications, SaaS platforms, unmanaged devices, IoT systems, BYOD assets, AI tools, and encrypted traffic create blind spots that traditional endpoint security cannot see.

Without web traffic visibility, organizations are making security decisions with incomplete information.

SWG + EDR

SWG does not replace endpoint security—it extends it.

EDR & XDR	Cloud SWG
Monitors endpoint behavior	Inspects web traffic before delivery
Detects threats on managed devices	Blocks threats before they reach devices
Investigates endpoint activity	Monitors cloud and web activity
Protects managed assets	Protects managed and unmanaged assets

RESULT: **Complete visibility across users, devices, applications, and networks**

The Visibility Gap

- Unmanaged devices cannot run security agents
- Cloud-to-cloud communications bypass endpoints
- Shadow IT and Shadow AI operate outside endpoint visibility
- Encrypted traffic conceals threats and data movement

RESULT: **Endpoint coverage does not equal risk coverage**

SWG Inspection Life Cycle

1. **Inspect** — What traffic is moving?
2. **Analyze** — What risks, data exposures, or policy violations exist?
3. **Enforce** — What should be allowed, restricted, or blocked?
4. **Protect** — Prevent threats, data loss, and unnecessary alerts

RESULT: **Continuous visibility and policy enforcement**

What's at Stake

- **Security Risk** — Threats hidden within encrypted and uninspected traffic
- **Data Loss** — Sensitive info exposed through sanctioned and unsanctioned services
- **Compliance Risk** — Limited ability to enforce, validate, and demonstrate policy compliance
- **Operational Burden** — Alert fatigue and time-consuming investigations
- **Business Impact** — Loss of trust, intellectual property, and competitive advantage

Cloud SWG Capabilities

- Enforce data loss prevention policies
- Control AI & SaaS application usage
- Discover cloud applications and shadow IT
- Support zero trust access strategies
- Block malicious destinations and downloads
- Enable remote browser isolation
- Inspect encrypted TLS traffic
- Generate forensic and compliance evidence

Business Outcomes

- **Reduced Risk** — Threats stopped before reaching endpoints
- **Lower SOC Workload** — Fewer alerts requiring investigation
- **Improved Governance** — Visibility into SaaS, AI, and web usage
- **Faster Investigations** — Network-level evidence for incident response
- **Stronger Compliance** — Continuous monitoring and policy enforcement
- **SSE Readiness** — Foundation for modern Security Service Edge architectures

Bottom Line for Executives

Endpoint security remains essential, but it cannot provide complete visibility into today's distributed environments. Secure Web Gateway technology closes critical visibility gaps by inspecting web traffic before threats reach endpoints, extending protection to unmanaged devices and cloud services, and providing the visibility required for effective governance, compliance, and risk management.

Organizations that combine endpoint security with web traffic inspection gain a more complete view of their environment, reduce operational burden on security teams, and establish the foundation for a modern Security Service Edge (SSE) strategy.

BROADCOM

SANS | Research Program