BROADCOM

Executive Summary

The Strategic Case for Web Traffic Inspection Beyond the Endpoint

Endpoint security has earned its place. EDR and XDR platforms are the most mature, most heavily funded layer of defense at most organizations, and they deliver real visibility into what happens on managed devices: process activity, file changes, behavioral anomalies. That part works.

The problem is everything else. A growing share of enterprise traffic never touches a managed endpoint at all: cloud applications, SaaS-to-SaaS communication, unmanaged and IoT devices, BYOD assets, and encrypted sessions that move across the network without passing through any agent. The average enterprise now runs 342 SaaS applications, and more than 95% of web traffic is encrypted. Much of it is invisible to endpoint tools by design.

This creates the quiet but costly assumption that endpoint coverage equals risk coverage. It does not. When the dashboards are green and deployment numbers are high, the environment feels protected, and the traffic that falls outside the agent's view is exactly where threats, data exposure, shadow IT, and compliance gaps accumulate. Attackers look for those paths on purpose.

A Secure Web Gateway (SWG) closes the gap by operating independently of the device. It inspects and enforces policy on web traffic before that traffic reaches an endpoint or leaves the organization, which means it sees managed and unmanaged assets alike. The operational difference is larger than it looks. A threat blocked at the gateway is a log entry. The same threat caught at the endpoint is an alert, a ticket, and an analyst's afternoon.

At its core, SWG is a visibility and control layer. It decrypts and inspects encrypted traffic, blocks malicious destinations, governs cloud and AI application usage, enforces acceptable-use policy, and keeps sensitive data from leaving through sanctioned and unsanctioned channels alike. It does not replace endpoint security. It extends protection into the areas that endpoint tools were never built to reach.

Leading organizations have stopped equating managed-device coverage with security. By folding secure web gateway capabilities into their architecture, they reduce risk, strengthen compliance, and lay the foundation for a modern Security Service Edge (SSE) strategy.

The Endpoint Visibility Gap

A growing share of enterprise traffic bypasses managed endpoints entirely

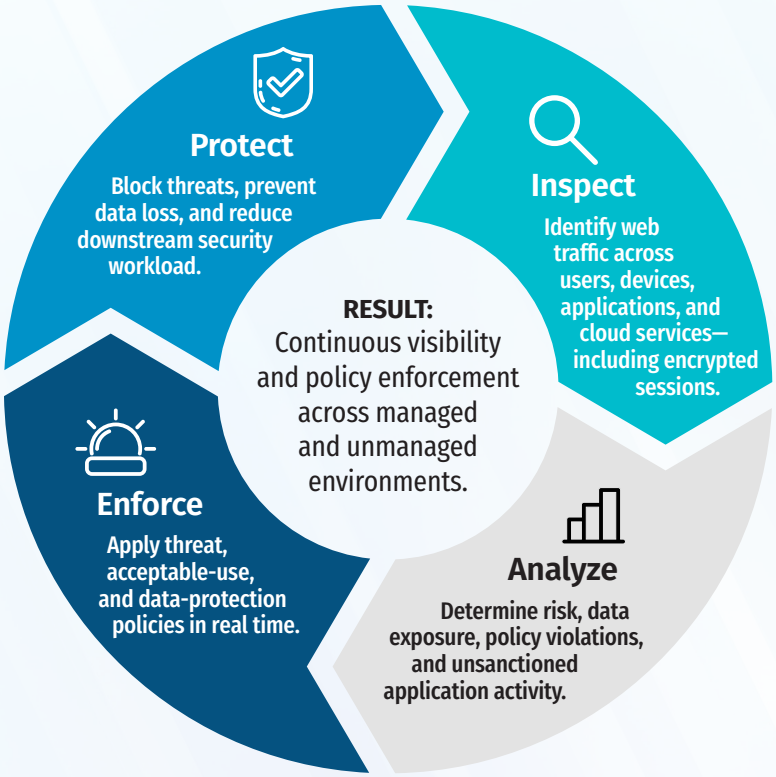
Unmanaged and IoT devices cannot run endpoint agents, and now outnumber managed devices on many networks

Cloud-to-cloud and SaaS communications occur with no endpoint in the path

With 95% of traffic encrypted, anything left undecrypted is invisible

RESULT:
You can't defend what you can't see

The Web Visibility Life Cycle



Key Capabilities of Cloud SWG

- TLS/SSL inspection and encrypted-traffic visibility
- URL filtering and reputation-based threat blocking
- Inline data loss prevention (DLP)
- Cloud and AI application discovery and governance (CASB)
- Threat intelligence, sandboxing, and malware inspection
- Coverage for managed, unmanaged, and remote users

SWG Bolsters Existing Security Investments

- Extends visibility beyond EDR and XDR
- Reduces the volume of low-value alerts reaching the SOC
- Strengthens cloud governance and compliance programs
- Supports zero trust and SSE initiatives
- Gives incident responders an independent forensic record

Bottom Line for Executives

Endpoint security remains essential. It simply cannot see the whole environment anymore. A secure web gateway closes the gaps endpoint tools were never designed to cover, reducing risk, improving compliance, and giving the security team a clearer picture of what is actually happening. It is also the foundation every other modern web and cloud control builds on. The first move is small: Turn on web traffic inspection and start seeing what you've been missing.

What's at Stake

Security Risk

Attackers exploit unmanaged devices, encrypted traffic, and unseen web activity, often remaining undetected until damage has occurred.

Data Loss

Sensitive information—including customer data, intellectual property, and content entered into AI tools—can leave through sanctioned and unsanctioned services.

Compliance Risk

Limited visibility makes it difficult to enforce, validate, and demonstrate adherence to regulatory and corporate policies.

Operational Burden

Security teams spend valuable time investigating threats that could have been blocked earlier in the traffic flow.

Business Impact

The combined effect is increased risk, higher operational costs, reduced trust, and potential loss of competitive advantage.

SANS | Research Program