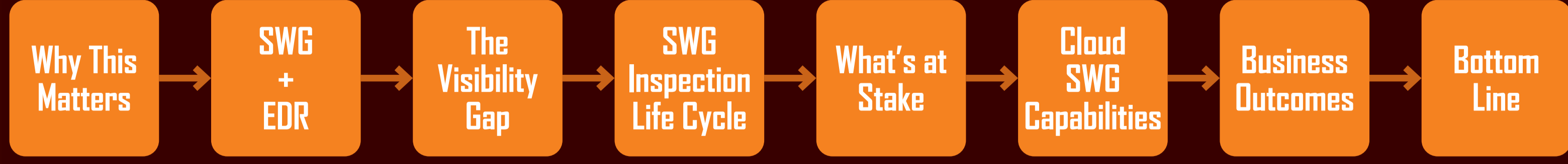


The Strategic Case for Web Traffic Inspection Beyond the Endpoint

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



Key Topics



Why This Matters

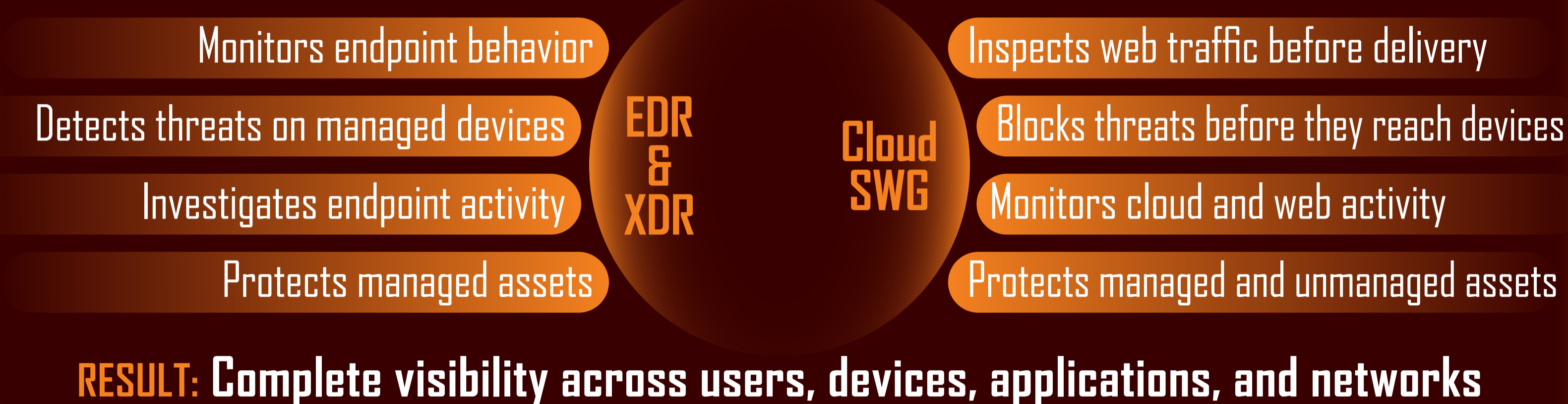
Organizations have invested heavily in endpoint security, but a growing percentage of enterprise traffic never reaches systems monitored by endpoint agents.

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.



The Visibility Gap



RESULT: Endpoint coverage does not equal risk coverage

SWG Inspection Life Cycle



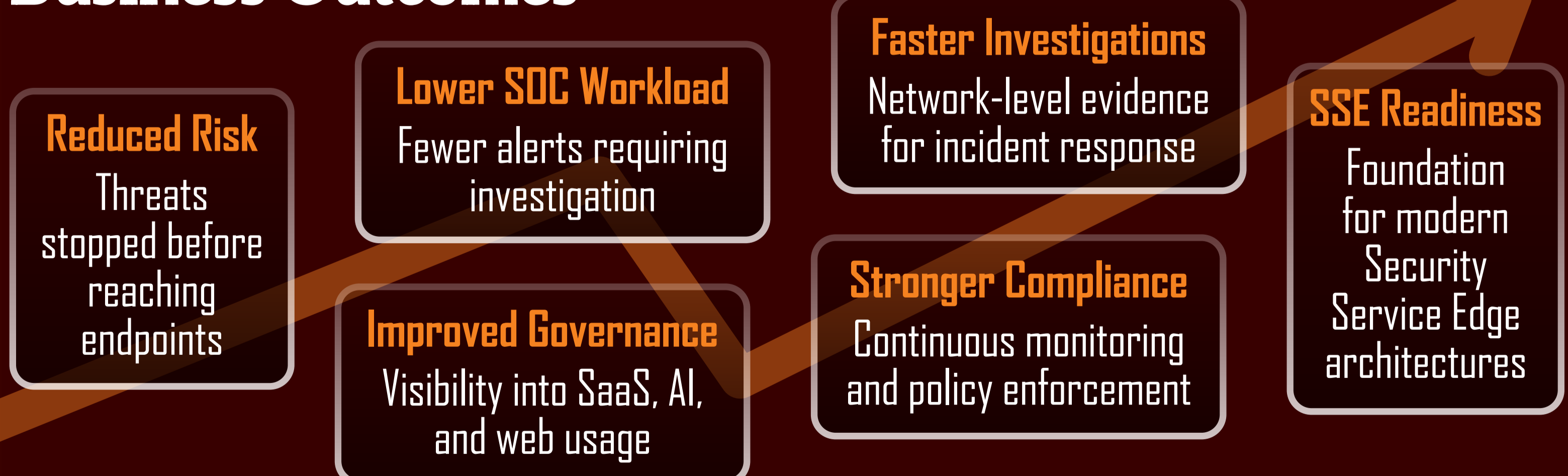
What's at Stake



Cloud SWG Capabilities



Business Outcomes



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.