SmartEdge Secure Web Gateway

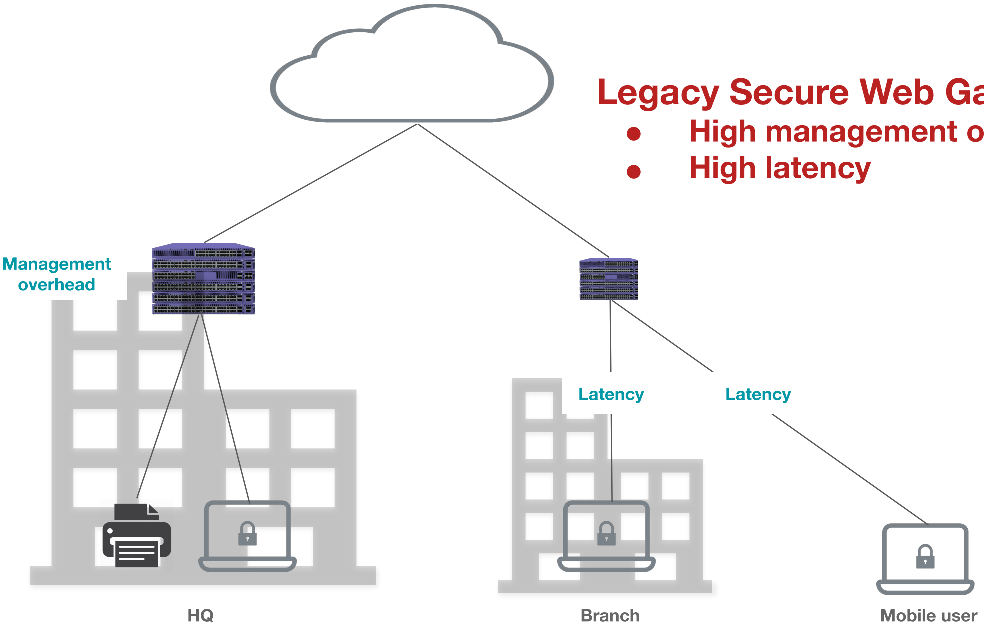
Technical Brief

Enterprises migrate their applications and data to the cloud for flexibility and cost savings. These advantages have resulted in mass adoption of cloud applications, but public cloud security concerns persist, leading enterprises towards third party security technologies.

Legacy SWG

Secure Web Gateways (SWG) have been available for years from legacy network security vendors. These solutions, offering a combination of premises appliances and passive endpoint agents to inspect network security for users in the office or on the go were designed with premises applications and managed endpoints in mind. Unfortunately, the move to public cloud applications and the need to secure unmanaged devices have rendered these architectures obsolete.

Legacy Approach	Notes
Appliance + Passive Endpoint Agent (Legacy vendors)	• Inelastic appliances handle bulk of traffic • Expensive to manage and upgrade • High costs and high latency



Legacy Secure Web Gateway

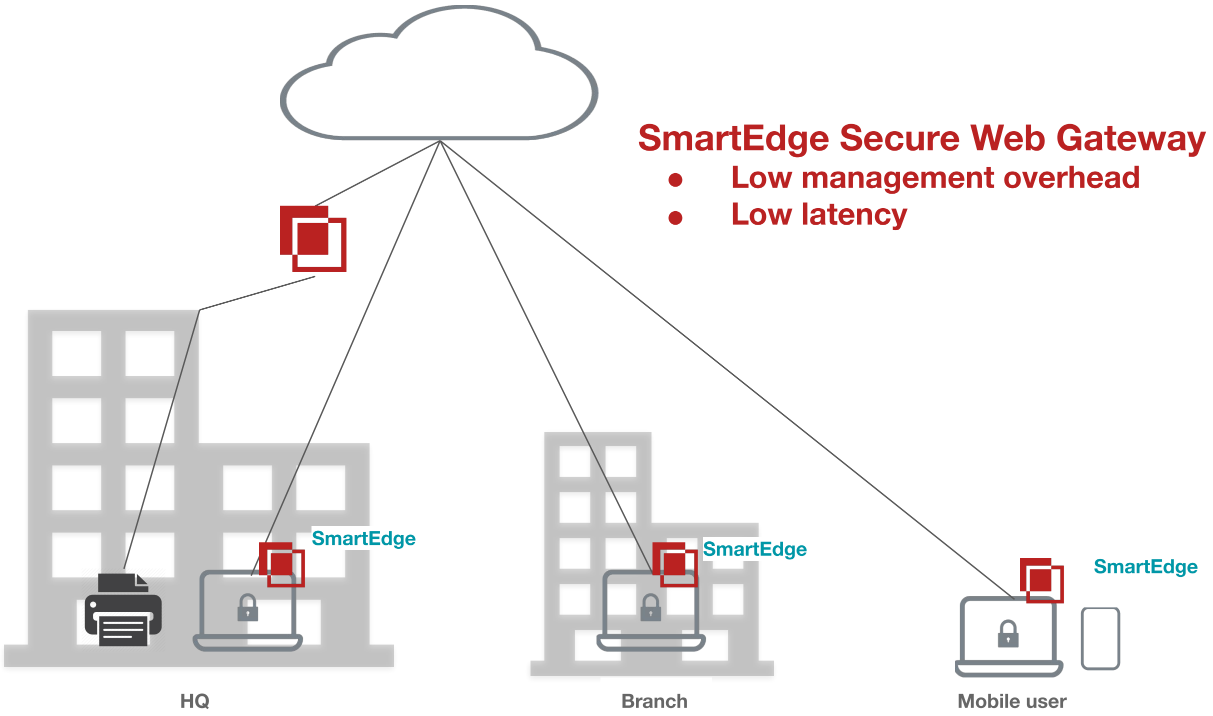
- **High management overhead**
- **High latency**

SmartEdge SWG

Bitglass SmartEdge Secure Web Gateway delivers the flexibility and low management overhead of a 100% cloud solution, while eliminating latency entirely for most traffic. SmartEdge is designed to be 100% cloud in combination with a smart endpoint agent. Mobile endpoints carry their own on-device SWG, locally terminating SSL and inspecting all network activity for blocking threats and data leakage.

Next-Gen Approach	Notes
Smart Endpoint Agent + Cloud proxy (Bitglass)	● Elastic cloud ● No appliances to manage and upgrade ● Intelligent endpoint agents handle bulk of traffic ● Low cost and low latency

Previously, it was infeasible to install the SWG on the endpoint, as SSL decryption requires the private key and the associated public key certificate signed by the enterprise. In such a situation, if any one endpoint is lost or stolen, all endpoints in the enterprise may be subject to man-in-the-middle attacks. Bitglass patent-pending trapdoor proxy technology overcomes this limitation and powers SmartEdge with trapdoor proxy agents to safely deliver low latency network security capabilities at a low cost.



SmartEdge Secure Web Gateway

- **Low management overhead**
- **Low latency**

Privacy and Compliance

With first gen SWG, the user suffers a loss of privacy since all the traffic is routed, decrypted and inspected at an appliance in the cloud. With the SmartEdge SWG, decryption and encryption happens on the endpoint. Only security events need to be logged and uploaded to the cloud.

Integrated CASB & SWG

With SmartEdge, enterprises enjoy the combined benefits of a SWG and Next-Gen CASB as a complete cloud security solution for any device - fixed devices behind the firewall, laptops on the move, and mobile phones and tablets.

Features	Benefits
Smart endpoint agent	Low latency protection for end-user devices
Cloud proxy	Protection for fixed assets, e.g printers
Full SSL decryption & inspection	Threat protection
DLP	Prevent data leakage to unmanaged apps
URL filtering	Block undesirable content
CASB integration	Security for managed and unmanaged cloud applications, e.g Office365, G Suite, ServiceNow, Slack, WorkDay...