# SmartEdge Secure Web Gateway

Data Sheet

The web is simultaneously an indispensable asset and a breeding ground for threats. Users can easily wander into domains where they can be infected with malware, become victims of credential compromise, or leak sensitive data. Users may simply access content that falls outside of accessible use policies, as well. Up to this point, only two approaches have been available to address these challenges.

Traditionally, SWGs have relied upon hardware appliances that are installed on premises. These appliances decrypt and inspect HTTPS traffic in order to prevent users from accessing dangerous or inappropriate websites. However, with this approach, remote workers and BYO devices must VPN back to the home infrastructure; creating latency and bottlenecks that degrade user experience, productivity, and efficiency. Architectures that require VPNs are not appropriate for modern business and can counteract many of the dynamism benefits that cloud and BYOD provide. In addition to these issues, appliances require extensive maintenance and can quickly become bottlenecks when user traffic surges--a concern for growing companies.

Other SWGs rely upon backhaul cloud proxies in order to provide web security. A simple agent on the endpoint forwards traffic to the cloud proxy for decryption and inspection. While this approach forgoes the use of a hardware appliance and can secure off-premises devices, the network hop still adds latency and harms the user experience. Additionally, user privacy is invaded as all traffic is inspected at the cloud proxy--there is no distinction between personal and corporate activity. These architectures can also endanger private keys and entail manual certificate management.

## Reimagining Web Security

Until now, organizations were essentially forced to choose between two approaches that are fundamentally flawed; both are characterized by performance bottlenecks, latency, and compromised user privacy. What if there were a better way to architect a secure web gateway? If a solution could avoid on-premises appliances and backhauling traffic by performing HTTPS decryption and inspection closer to the user, then it could avoid a network hop, deliver enhanced performance, and improve the user experience.

Having web security that is integrated with the rest of the cloud security stack is also key for modern enterprises. Rather than configuring multiple, disjointed policies for complementary solutions like SWGs and cloud access security brokers (CASBs), organizations need a single platform that encompasses both and can protect data wherever it goes. Consider, for example, when CASBs are used to prevent the sending of sensitive data via email in the Outlook app, but no SWG (or SWG policy) is in place to protect the same data when a user tries to share it through Yahoo Mail in a web browser. Ideally, a single platform will integrate CASB and SWG, protecting sensitive data in any environment through consistent policies.

The importance of these issues is why Gartner has predicted the rise of the secure access service edge (SASE), which involves the consolidation of network and cloud security solutions into cloud-delivered platforms.

## The Bitglass Solution

Bitglass' SmartEdge Secure Web Gateway disrupts the status quo and eliminates these longstanding issues by deploying at the ultimate edge, on users' devices. As the industry's only on-device SWG, Bitglass decrypts and inspects traffic directly on users' endpoints, providing a host of novel benefits.

The edge-based architecture eliminates the need for VPNs and backhauling traffic to cloud proxies and on-premises appliances. This reduces latency and enhances the user experience while ensuring consistent, scalable web security in times when traffic surges would overwhelm architectures that rely upon a single bottleneck inspection point to handle all traffic.

SmartEdge also overcomes the privacy concerns associated with typical SWG architectures. Rather than sending all traffic to an appliance or cloud proxy, Bitglass' solution decrypts and inspects HTTPS traffic directly on users' devices. As relevant logs are generated and uploaded to the cloud only when security policies are violated, this means that personal traffic remains safe on users' devices. In other words, users' personal credentials, activities, and information are left on the endpoint and are not caught in the corporate dragnet in the name of cybersecurity.

Bitglass provides its SmartEdge SWG along with its Next-Gen CASB and its zero trust network access (ZTNA) as an integrated, three-pronged SASE offering that leverages a single dashboard and a consistent set of policies for comprehensive security. With the Bitglass Total Cloud Security Platform, sensitive data patterns can be detected and protected consistently wherever they go--whether users are trying to steal data from on-premises applications, exfiltrate it through the web, or share it with a third party through SaaS. By using Bitglass, customers can avoid the interoperability, management, and consistency concerns that abound when using disjointed solutions from different vendors.

## Product Details

The SmartEdge SWG controls access to content through a broad set of granular attributes. Preset policies automatically filter URLs and shadow IT, allowing or blocking them for specific user groups, device types, and geographical locations. Content can be controlled based on category (e.g. malware sites, gambling, pornography, and dozens more) as well as by trust score. If an organization wants to control shadow IT through a different tool or enforcement point, Bitglass' closed-loop discovery provides exportable, dynamically generated app lists that can be customized by app category, trustworthiness, and more.

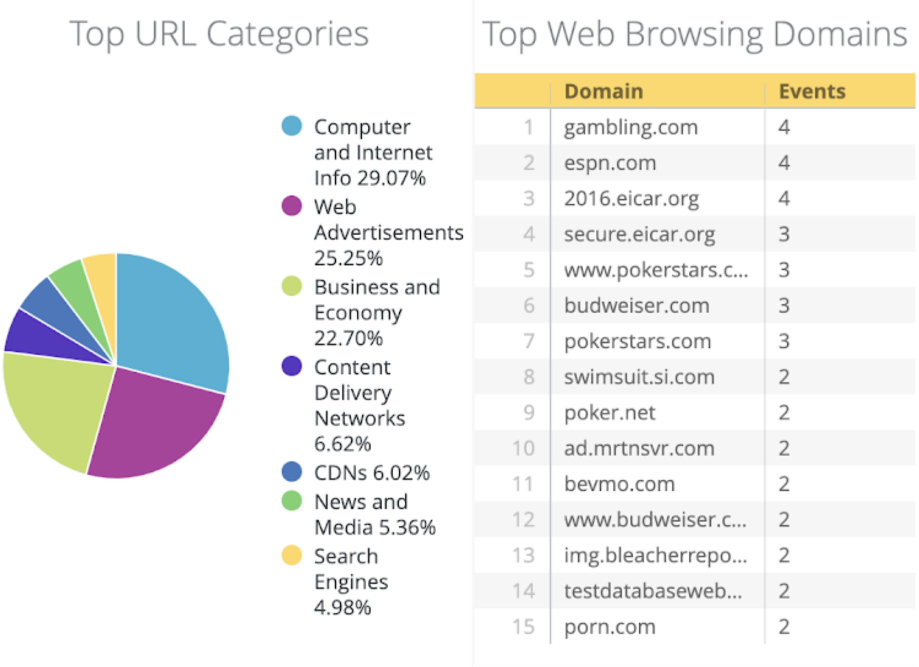
As the web contains a myriad of files infected with malware, the SmartEdge SWG provides advanced threat protection that scans documents for threats on download. CrowdStrike, Bitdefender, and Cylance engines are baked directly into Bitglass' solutions, and customers can choose one or more to detect and halt known and zero-day malware in real time.

When organizations want a layered approach to web security, they can also leverage remote browser isolation (RBI), which defends against malicious JavaScript and threats like drive-by downloads. RBI isolates website sessions in the cloud and presents users with a virtual session (a browser within a browser) so that no code is executed directly on a user's device itself.

By integrating application access and web security into a single platform, uniform data loss prevention (DLP) policies can be enforced across SaaS applications, custom applications, and web applications or websites. If a user attempts an unauthorized upload of sensitive information to a website or unmanaged application, the leakage will automatically be prevented.

When users violate a policy and have an upload of data or access to content blocked, they can be alerted with a custom message via email, an inline popup, or both, so that they can be made aware of why the action was denied.

Bitglass' SWG is deployed via a SmartEdge agent that is installed on users' endpoints to terminate HTTPS and inspect traffic locally (Bitglass also has a cloud-proxy SWG when agents aren't feasible). When preset policies are violated, the agent automatically blocks access to content directly on the device. Logs relevant to the security incident are then uploaded to the cloud so that they can be viewed in Bitglass' dashboard for more detail. Summary information is also provided; two examples are shown in Figure 1.


Top URL Categories
Computer and Internet Info 29.07%
Web Advertisements 25.25%
Business and Economy 22.70%
Content Delivery Networks 6.62%
CDNs 6.02%
News and Media 5.36%
Search Engines 4.98%

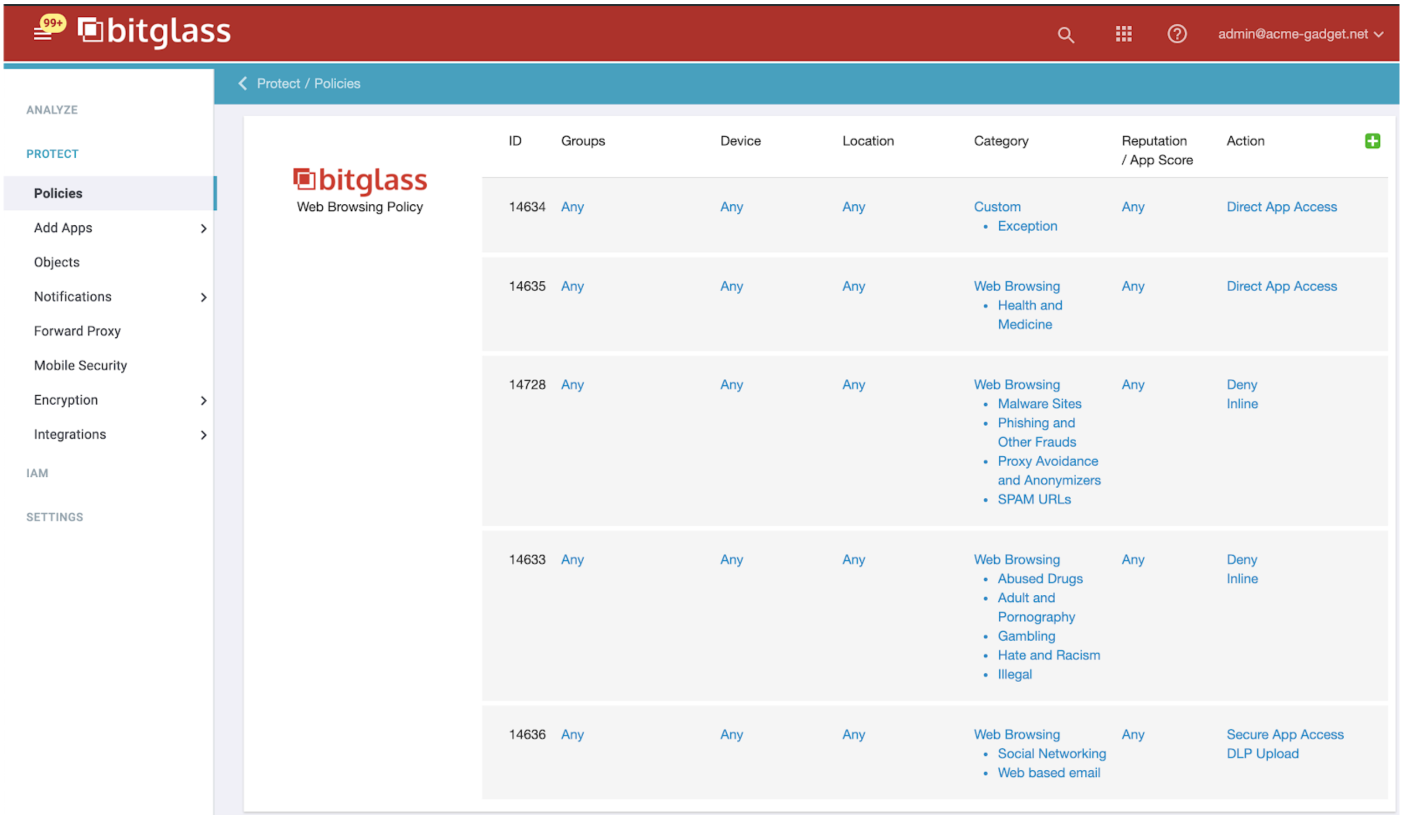
Top Web Browsing Domains

| | Domain | Events |
|---|---|---|
| 1 | gambling.com | 4 |
| 2 | espn.com | 4 |
| 3 | 2016.eicar.org | 4 |
| 4 | secure.eicar.org | 3 |
| 5 | www.pokerstars.c... | 3 |
| 6 | budweiser.com | 3 |
| 7 | pokerstars.com | 3 |
| 8 | swimsuit.si.com | 2 |
| 9 | poker.net | 2 |
| 10 | ad.mrtnsvr.com | 2 |
| 11 | bevmo.com | 2 |
| 12 | www.budweiser.c... | 2 |
| 13 | img.bleacherrepo... | 2 |
| 14 | testdatabaseweb... | 2 |
| 15 | porn.com | 2 |

Figure 1: Charts from the Bitglass dashboard

Bitglass' patent-pending Trapdoor Proxy technology ensures secure key management on the endpoint; the agent on each device serves as its certificate authority. Bitglass automatically manages the creation, storage, and revocation of certificates on all devices using SmartEdge, saving time and energy for admins who would otherwise have to manage certificates manually. This also means that even if one device is stolen or compromised, it cannot be used to mount man-in-the-middle attacks against other user devices.

Setting SWG policies in the Bitglass dashboard is simple. As shown in Figure 2, admins merely configure each of the six columns to suit their needs. They just need to identify the user groups, devices, and locations for which they would like policies to be enforced, select the categories and trust ratings of content that they would like to filter, and decide how they would like notifications to be presented to end users.



| ID | Groups | Device | Location | Category | Reputation / App Score | Action |
|---|---|---|---|---|---|---|
| 14634 | Any | Any | Any | Custom<br>• Exception | Any | Direct App Access |
| 14635 | Any | Any | Any | Web Browsing<br>• Health and Medicine | Any | Direct App Access |
| 14728 | Any | Any | Any | Web Browsing<br>• Malware Sites<br>• Phishing and Other Frauds<br>• Proxy Avoidance and Anonymizers<br>• SPAM URLs | Any | Deny<br>Inline |
| 14633 | Any | Any | Any | Web Browsing<br>• Abused Drugs<br>• Adult and Pornography<br>• Gambling<br>• Hate and Racism<br>• Illegal | Any | Deny<br>Inline |
| 14636 | Any | Any | Any | Web Browsing<br>• Social Networking<br>• Web based email | Any | Secure App Access<br>DLP Upload |

Figure 2: Configuration of web security policies in the Bitglass dashboard

## SmartEdge SWG Key Features

| Requirement | Summary of Capability |
|---|---|
| **Availability and Performance** | • 99.99% uptime since 2014.<br>• On-device SWG reduces latency and streamlines user experience.<br>• Automatic certificate management directly on each endpoint.<br>• Forgoes legacy, appliance-based deployments. |
| **URL Filtering and Threat Protection** | • Control access to domains by dozens of categories, including bot nets, malware sites, phishing sites, streaming media, violence, drugs, hate and racism, pornography, and gambling (powered by Webroot).<br>• Use remote browser isolation to defend against threats like drive-by downloads.<br>• Scan file downloads from the web in real time to halt malware; leverage CrowdStrike, Bitdefender, or Cylance engines. |
| **Controlling Shadow IT** | • Leverage Bitglass' shadow IT library of over 600k apps.<br>• Block access based on dozens of categories like file sharing, sports, video chat, messaging, and social network.<br>• Closed loop discovery provides exportable app lists for third-party tools serving as shadow IT control points. |
| **Trust Scoring** | • Allow or block access to content based on whether it is less than, equal to, or greater than trust scores of your choosing. |
| **Data Loss Prevention** | • Elastic DLP uses keywords, regular expressions, proximity, pattern match counting, logical/Boolean operators, metadata attribute extraction, exact data matching, OCR, fingerprinting, and multiple language support. |
| **User Privacy** | • Traffic is decrypted and inspected directly on endpoints.<br>• Only security events are logged and uploaded to the cloud. |
| **Flexible Licensing** | • SmartEdge is licensed by the number of users, not by the number of devices or data volume. |
| **Secure Access Service Edge** | • The SmartEdge SWG is one component of Bitglass' SASE offering.<br>• Further enhance security with Bitglass' Next-Gen CASB and agentless ZTNA. |
| **Alternative Deployment Options** | • Bitglass also offers a cloud-proxy SWG for when agent installations on users' devices are not feasible; for example, IoT or personal endpoints.<br>• GRE tunnels ensure enhanced performance. |