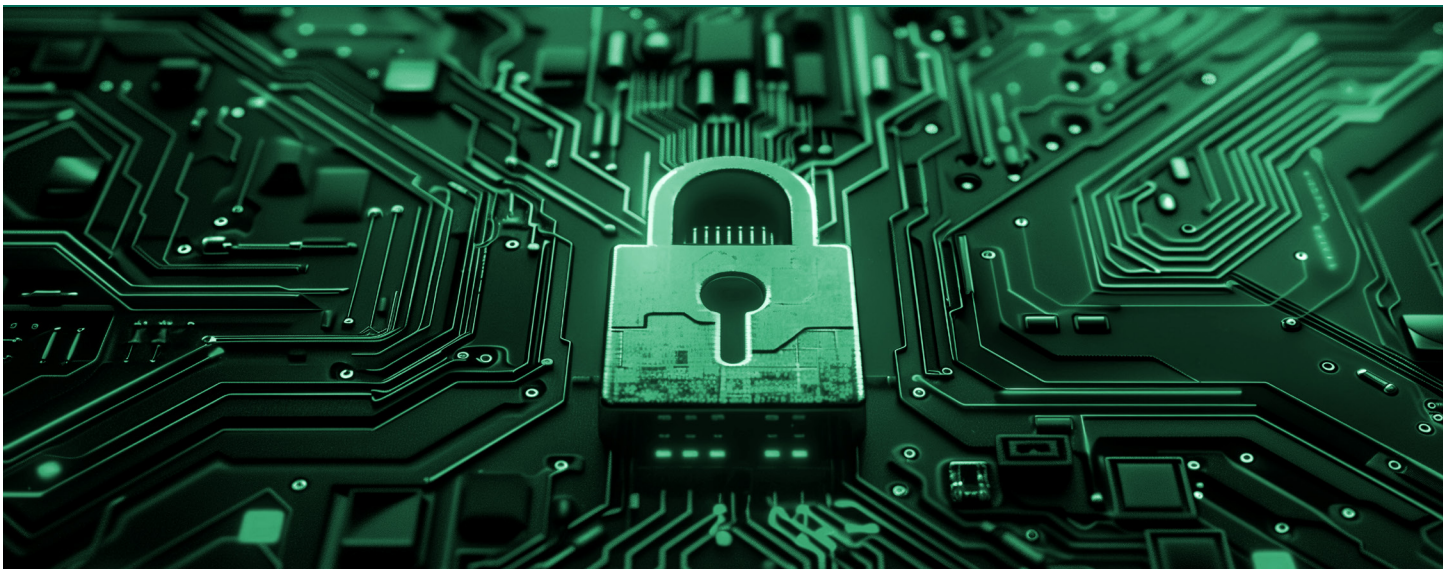
FORTRA

DATASHEET (FORTRA)

5 Ways SWG Keeps Users and Data Safe Online



The internet has revolutionized workforce productivity and collaboration. Your employees rely on connectivity to excel at their jobs, accessing the corporate network, communication tools, and other resources from multiple locations and devices. Enabling secure connectivity without hindering the end-user experience has become a top priority for most IT security teams.

The need for a modern SWG

Secure web gateways (SWGs) were created to help filter internet traffic, protect against malicious web content, and enforce corporate and regulatory policy compliance for all internet users. While SWGs are not a new technology, they have evolved from their origins as on-premises web proxies and now deliver more robust, cloud-based web security to stay ahead of today's sophisticated internet threats.

Modern SWGs provide multiple layers of protection, playing a crucial role in stopping advanced internet threats like malware and phishing while also preventing the loss of sensitive data on the web.

Let's take a deeper look at the top 5 capabilities that SWGs provide to keep users and data safe online:

1. Control website access

SWGs include URL and content filtering that inspects web traffic in real time, blocking access to unauthorized websites and malicious content. SWGs control access to websites based on reputation, category, and defined acceptable use policies, blocking access to sites when they are deemed unsafe or inappropriate. This reduces the risk of users visiting phishing sites or inadvertently downloading harmful files.

2. Prevent data loss on the web

Many SWGs include built-in data loss prevention (DLP) capabilities that scan data uploads for sensitive information, helping to prevent the accidental or intentional sharing ofconfidential data. This has become even more important with the rise in usage of GenAI and social networking sites. Data submitted or shared by employees on these sites may include software source code, financial information, personally identifiable information (PII), or other confidential data, and a SWG can identify this to prevent data leakage.

3. Protect against zero-day threats

SWGs use advanced techniques such as real-time traffic inspection, malware scanning, and sandboxing to detect and block malicious content like malware or phishing attacks. This prevents threats from reaching users' devices and entering the corporate network. Remote browser isolation (RBI) creates further protection against zero-day threats by isolating browsing sessions in a secure, cloud-based environment. This is particularly important when users visit a new or unclassified site, preventing malicious content from reaching the user's device and minimizing the risk of data exfiltration.

4. Inspect all web traffic

Acting as a next-gen firewall, SWGs can natively inspect incoming and outgoing traffic across all ports and protocols to pinpoint potential threats and detect malware hidden in encrypted traffic. After scanning for malware or other risks, the traffic is then re-encrypted and allowed to proceed safely. This prevents attackers from using encrypted channels to bypass security. If malware is detected, it is blocked, quarantined, and notification is sent to the user and admin.

5. Monitor and control user activity

SWGs continuously monitor user activities, such as web browsing, file uploads, and form submissions, providing

detailed logs as well as alerts for suspicious behavior. SWGs help to identify and manage shadow IT, providing visibility into unsanctioned devices and apps that are connecting to the internet from the corporate network and enforcing policies that limit or block the use of unsanctioned cloud applications.

Protect against internet threats and data leakage with Lookout Secure Internet Access

Fortra SWG is built on the principles of zero trust SWG built on the principles of zero trust, protecting users, devices, networks, and data from internet-based threats. Secure Internet Access not only stops online zero-day threats, but it also prevents data leakage to websites and monitors web activity to detect and control shadow IT.

To learn more about Fortra and our Cloud Data Protection product line, visit Fortra.com.

FORTRA

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.

Copyright © Fortra, LLC and its group of companies. Fortra®, the Fortra® logos, and other identified marks are proprietary trademarks of Fortra, LLC. (fta-cdp-ds-0525-r1-an)