FORTRA

DATASHEET (CLOUD DATA PROTECTION)

Fortra SWG

Protect your organization and data from internet threats

Fortra SWG is a cloud-delivered secure web gateway and Firewall as a Service (FWaaS) that is part of the data-centric cloud security tool set from Fortra. Built on the principles of zero trust, it protects users, underlying networks, and corporate data from internet-based threats while also preventing data leakage. With a single-proxy architecture, it also offers security controls for web and non-web traffic, and the ability to inspect all incoming and outgoing web traffic for malicious content and sensitive data.

With a streamlined, always-on security, SWG simplifies IT operations, and provides better user experience.

Challenges

The concept of network security has turned inside out. With apps and data residing in the cloud and users connecting from anywhere, IT has lost the visibility and control they had with perimeter-based tools. Below are the challenges IT organizations are facing as a result.

Lack of protection against phishing attacks and malicious content

Organizations with highly sensitive information are attractive targets of sophisticated cyber threats, such as ransomware attacks. Bad actors typically leverage phishing attacks to trick users into providing login credentials to the corporate environment.

With credentials in hand, attackers can penetrate an organization's network and execute malicious code to encrypt or exfiltrate sensitive data. Without comprehensive phishing protection against all phishing methods — including SMS, email, messaging apps, and web apps — organizations remain exposed and are more likely to suffer a breach.

Unsanctioned apps add hard-to-detect shadow IT risk

The risk of shadow IT and unsanctioned apps has never been greater. Cloud services such as file storage, messaging, and video solutions, while designed for consumers, offer a convenient option for work tasks as well. Unfortunately, on-premises web gateway solutions are unable to detect them, introducing the potential for data leakage that goes undetected.

PRODUCT SUMMARY

Benefits

- Protect hybrid workforce from phishing and malicious content on the internet
- Provide URL and content filtering for secure internet access
- Enforce effective cloud governance and help achieve compliance
- Monitor and assess risk with web and cloud usage
- Protect corporate data stored in unsanctioned SaaS and cloud apps
- Improve end user experience with direct access to internet

Increase compliance risk from remote work

More than ever, employees are using the internet and web apps to get work done. They are bypassing perimeter-based security to connect directly to whatever they need, from any device and location. With company data spread across unsanctioned apps, websites and cloud vendors, it's difficult to get comprehensive visibility into your data and apps. This creates countless channels for attackers to steal data or distribute malware. It also increases the potential for mishandling sensitive data, resulting in compliance violations.

Costly and time-consuming maintenance

Managing a patchwork of disparate security solutions is inefficient. Each specialized tool requires valuable IT resources to configure and maintain each solution, including countless hours troubleshooting interoperability issues. On-premises SWGs complicate maintenance even further as it requires the manual upgrading of physical hardware across several data centers. This includes the need for technicians to go onsite, perform the installation, and test that all appliances are functioning properly.

Legacy gateways are slower and provide limited security

Organizations using on-premises SWG solutions must backhaul traffic through a data center in order to apply compliance and security policies. Excessive latency not only creates poor end user experiences, it also limits the range of security that can be applied to a data stream in real-time. For example, to block the upload of sensitive data to a website, a SWG needs to inspect data, apply policies, and take protection action all in one motion. A lag in throughput degrades effective detection and response and results in a poor user experience.

Benefits of Fortra SWG

As organizations transition from on-premises security tools to cloud-delivered services, or are looking to consolidate disparate cloud-based solutions, they need a platform that enables them to pace their migration.

As part of a cloud security strategy alongside tools such as CASB, Fortra SWG ensures that consistent policies are applied across all internet use cases — the same way they would be applied to SaaS apps and private enterprise apps. This provides organizations with a simpler way to manage and deploy security tools, monitor end user activity and enforce organizational policies such as Shadow IT.

Protect hybrid workforce from advanced internet-based threats

Fortra's single-proxy architecture enables organizations complete visibility of all end-user traffic whether it's happening on the internet, in SaaS apps or private enterprise apps. With a built-in Firewall as a Service, Fortra extends inspection of incoming and outgoing traffic to include all ports and protocols, enabling granular visibility and access control into non-web traffic. With this end-to-end visibility, IT can enforce policy controls on both sanctioned and unsanctioned apps to prevent unauthorized traffic from entering the corporate network.

URL filtering enables administrators to control which websites their employees, guest users, and shared devices can access based on threat intelligence from hundreds of millions of websites, domains and apps in our Security Graph. Fortra also integrates with multiple threat-intelligence engines to provide the latest threat signatures and information. This enables Fortra to detect and stop any internet-based attacks like ransomware, phishing, zero-day and browser-based threats.

Remote Browser Isolation (RBI) can add an additional layer of protection against zero day threats, malware downloads and other browser vulnerabilities. RBI enables Internet users to safely browse new or uncategorized websites by isolating potentially risky content in a cloud-hosted browser. Users, devices, and underlining networks remain secure while employees retain the freedom to collaborate, share information, and access web resources in order to be productive.

Enforce effective cloud governance and help achieve compliance

Users are often switching between corporate and personal instances of cloud apps. This means it's critical that you not only understand which instance is being used, but be able to enforce data loss prevention (DLP) policies based on this information.

Fortra SWG provides data protection capabilities that reduces false positives and improve employee productivity. These actions include encrypting, watermarking, masking,

redacting, highlighting, setting expiration times, or allowing offline access. By detecting the destination of the data, SWG prevents it from being sent to unauthorized locations, apps or users that could put the organization in violation of compliance or data privacy laws.

Fortra SWG also offers adaptive access controls that are based on a user's risk score, device posture, and location for automatic enforcement of security policies that ensure compliance with local and industry regulations.

Monitor and assess risk with web and cloud usage

Fortra consolidates IT security infrastructure with a unified platform that delivers a single proxy, a single end user agent, and a single policy infrastructure. This eliminates the need for multiple IT security tools from different vendors, thereby reducing the risk of human errors and inconsistent policies.

Fortra performs TLS/SSL inspection on all inbound and outbound traffic passing through the our cloud security tools so that packet decryption and encryption only needs to happen once. This not only provides the visibility needed to apply protection policies but it also results in a smoother, faster end-user experience.

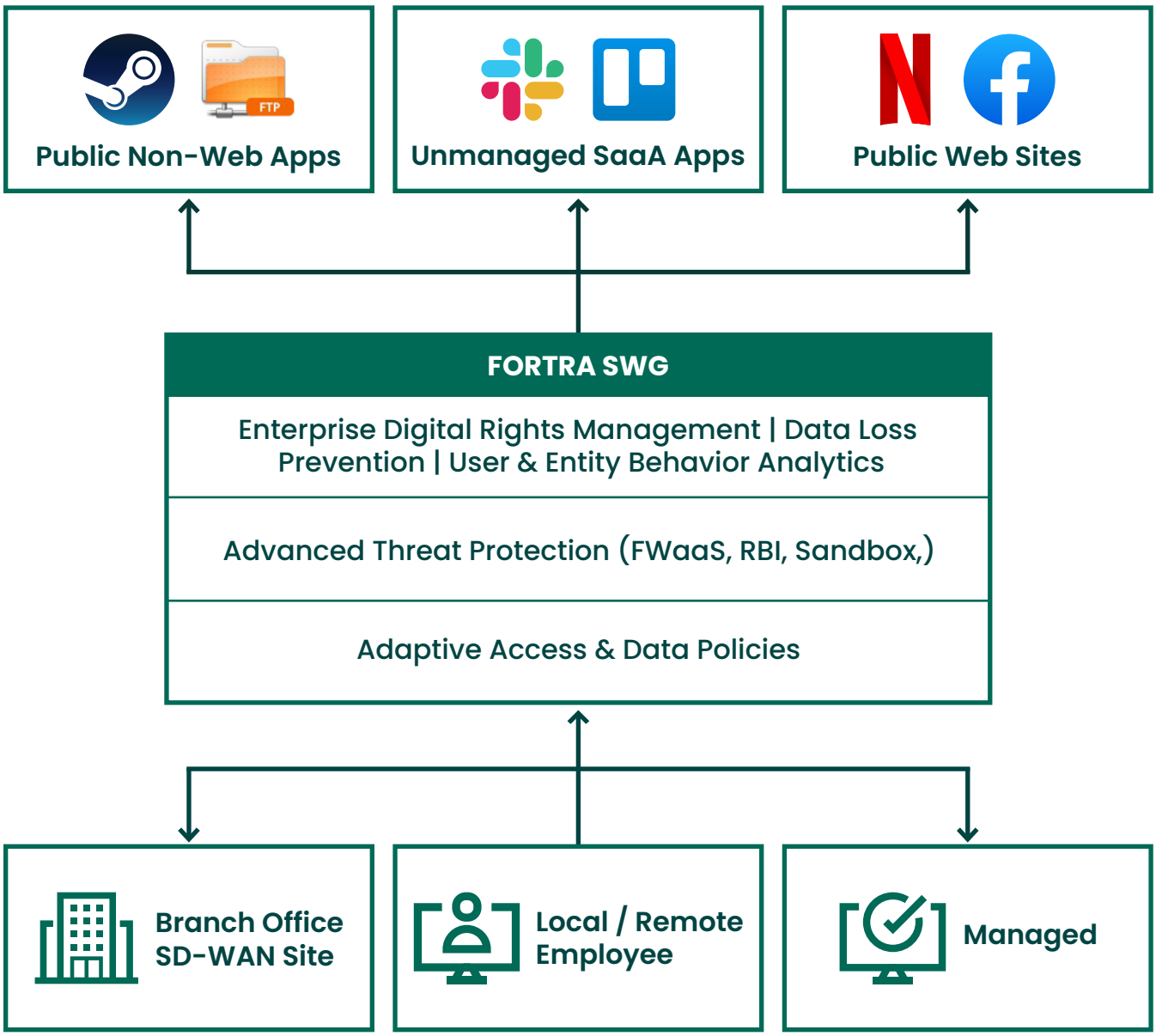
Protect corporate data stored in unsanctioned SaaS and cloud apps

By monitoring sensitive data across managed and unmanaged apps and websites, administrators get complete end-to-end visibility to ensure proper enforcement of data protection policies. Fortra SWG leverages industry-leading intelligence gathered from over 27,000 apps, enabling it to identify shadow IT as users are connecting to unauthorized apps or personal accounts. This ensures real-time threat protection.

Fortra SWG leverages industry-leading intelligence gathered from over 27,000 apps, enabling it to identify shadow IT as users are connecting to unauthorized apps or personal accounts. This ensures real-time threat protection.

Improve end user experience with direct access to Internet

Unlike traditional solutions that backhaul traffic, Fortra SWG provides security controls closer to the users and apps by being delivered from the cloud. This proximity enables it to efficiently enforce security inline ensuring the end user has a seamless experience.



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.

