Forcepoint

Datasheet

Forcepoint Web Security

Key Benefits:

- 99.999% uptime SLA
- Smart steering pivots from web proxy to direct connection to minimize latency and maximize throughput without sacrificing security
- Multiple real-time content engines analyze full web page content, active scripts, web links, contextual profiles, files and executables for the ultimate protection
- SCIM provisioning accelerates user on-boarding
- Data-in-motion scanning blocks malware and data exfiltration between users and any web application, no matter where they are located.
- RBI with CDR enables safe use of unknown websites and safe use of files downloaded from those websites
- Controls website access down to the URL directory level
- SWG function cannot be bypassed or disabled by the user

Forcepoint Web Security provides guardrails for the safe use of any website, including granular controls for AI sites. Simplify enforcement of organizational policies to unlock productivity enhancements while mitigating risks from sensitive data exposure and ransomware.

Forcepoint Web Security Architecture

Forcepoint uses a distributed enforcement architecture so that organizations have more flexibility to meet changing business requirements. Forcepoint Web Security allows for enforcement using either the forward proxy (cloud, on-prem, or hybrid) for sites and branch offices or the unique agent-based proxy for managed devices. With the forward proxy, organizations can provide all users at sites, even guests and those on unmanaged devices, with reliable, safe web access as well as remote users on managed devices.

Locations can forward web traffic to the Forcepoint Web Security platform in the cloud using GRE or IPSEC tunnels, and those using Forcepoint FlexEdge Secure SD-WAN can use 'EasyConnect' to automatically connect sites to the cloud platform. The policy manager makes it easy to apply per-network policies that can be used across sites. For example, organizations can set up guest internet access to be isolated using the optional Forcepoint RBI service for the ultimate level of threat protection and easily apply this guest WI-FI policy to all locations. This option is ideal for branch offices and sites with public or customer WI-FI access, and Forcepoint also provides an ideal solution for remote workers on managed devices using agent-based Web Security.

Agent-based web security can use a PAC file to steer traffic to the cloud proxy, or enforce policies locally for the best possible web performance. With agent-based enforcement the user and company data are protected no matter where the user is located: at home, in the field, or in the office. By design, the Web Security agent cannot be stopped by the user or uninstalled by the user without approval from a Forcepoint administrator, thus ensuring its function is not easily bypassed by the user.

Forcepoint's distributed architecture provides global presence for low latency and optimized user experience. When the direct connect endpoint mode is used enforcement is performed on-device for the fastest possible user experience. This means web traffic can go straight to the site without first detouring through a proxy located in the cloud or at a branch office in figure 1.

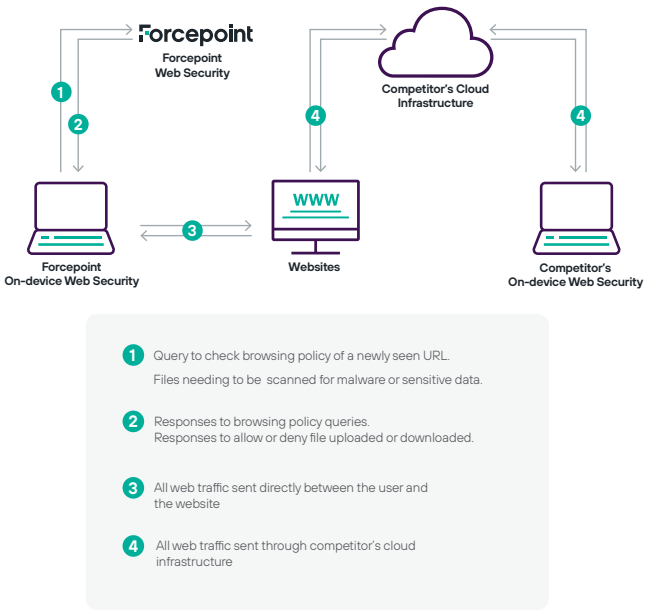

Figure 1: Forcepoint Web Security Traffic Routing vs. Competitors

As shown in the figure, Forcepoint Web Security's Direct Connect Endpoint mode, on the left, only needs to communicate with the Forcepoint backplane in two situations: when first attempting to access a website not recently visited to determine access restrictions, and when attempting to upload or download files or other data that needs to be scanned for malware or sensitive data.

By comparison, the other vendor's on-device SWG, on the right, must send all web traffic through the vendor's cloud backplane for traffic inspection and forwarding. This routing of all web traffic through the other vendor's cloud infrastructure can cause up to a 50% loss in effective throughput, thus causing productivity issues for users in low bandwidth locations. Because file uploads and downloads are a small fraction of overall internet traffic for most users, Forcepoint Web Security can typically support throughput of about 95% of total available internet bandwidth, while reducing latency, thus supporting greater user adoption.

Forcepoint Web Security Features

Granular content categories and policy options

Real-time categorization enables all web traffic to be easily controlled with highly granular web categories. For example, instead of having to treat all GenAI sites the same, multiple categories of GenAI sites means you can restrict access to sites meant for generating code while allowing more access to sites meant for generating images or conversation, all while enforcing guardrails to keep your sensitive data safe.

Real-time scanning

Forcepoint Web Security inspects traffic content in real-time to provide highly efficient and accurate web content categorization and scanning, without sacrificing performance. This enables organizations to easily enforce web access and usage controls tailored to their needs, including industry-leading threat prevention and easy-to-use data security. When new web content is seen the security scanning engine leverages ML to identify zero-day threats and block access. Forcepoint Web Security goes beyond DNS checks and IP reputation to mitigate risks in real-time—protecting against novel malware just as effectively as known malware and delivering reliably fast performance anywhere your users are.

Content inspection (DLP and malware)

Forcepoint Web Security can inspect encrypted web traffic to block the loss of sensitive data using our data inspection and classification engines. We make it easy to apply PCI, PHI, and PII controls right out of the box, to control password information and encrypted files all with the click of a button. Admins can also create custom patterns, phrases, dictionaries, and regular expressions as needed. Further, integration with Forcepoint's cloud or on-prem DLP enables you to inherit advanced DLP policies directly into Forcepoint Web Security.

RBI essentials

Today we often need access to new tools and new sites to do our jobs but more and more often there are parts of the web we just cannot trust. This is where a Zero-Trust approach to web access is needed. The SaaS version of Forcepoint Web Security comes with an included essential level of Remote Browser Isolation (RBI) to allow safe access to 'unknown' or newly registered sites which may host threats. RBI functions by rendering web traffic in an isolated and secured cloud environment, with the session streamed to the end user so nothing present on the web page ever touches the user's device and the browser and vm hosting it is simply deleted at the end of the session.

Analytics dashboard

Web productivity dashboards display graphical representation of web traffic data covering top requested categories, top filtering actions by request, top groups for blocked requests, top users for blocked requests, top social web channels, and top social web activities. Threat dashboards cover security events, threat types, security risk locations by source and destination, and top security risk sites, while bandwidth dashboards highlight bandwidth usage by web category, top connection IPs, top groups, sites, and top users.

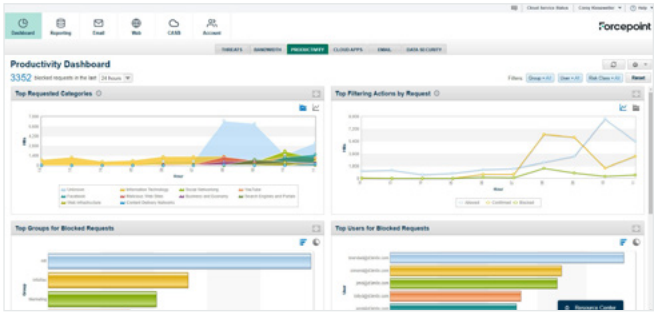

Figure 2: Productivity Dashboard

Web Security bypass prevention

Users cannot kill the Web Security processes on their Windows or MacOS device, and users cannot uninstall the on-device agent powering Forcepoint Web Security without assistance from the Forcepoint administrator.

The Cloud Apps dashboard surfaces information on cloud application usage and associated risk. This includes viewing cloud apps ranked by risk level and listed by cloud app, bandwidth, or user. Additional graphs include top cloud apps by hit count and by bandwidth, top cloud apps by category, top cloud apps by risk level, top cloud app users, and cloud app activity by category. The Bandwidth dashboard covers bandwidth usage by web category, connection IP, top groups, users and sites. And the Data Security dashboard displays DLP incidents over time, by content type, source and severity, top domains, and web categories.

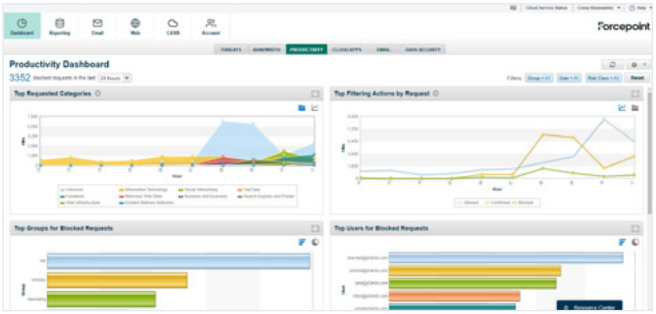

Figure 3: Threat Dashboard

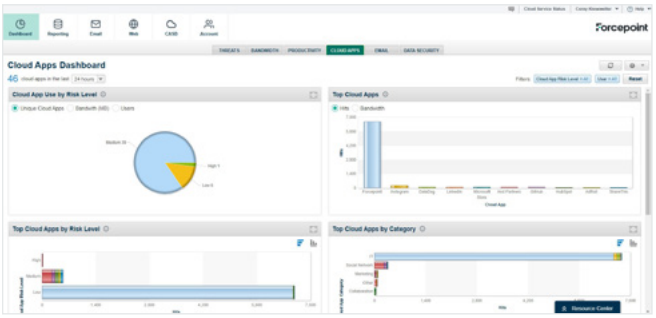

Figure 4: Cloud Apps Dashboard

FEATURES	BENEFIT
Web Control Capabilities	
Granular Web Access Controls	→ Allows finely tuned control of corporate web and cloud app use
Granular Social Media Controls	→ Controls permissible use of social media and distinguish between sections like mail, games, chat, posting, photo uploads, and more
Connection-based Policy Switching/Context Aware Policy Switching	→ Automatically adjust policy based on how and where the user is connecting from
Productivity Controls/Time Quotas	→ Enforce quotas on any web categories during business hours to help maintain productivity
Single Sign On	→ Integrate with SSO providers like Okta or Ping Identity to enforce even stronger identity-based access controls
Data Protection Capabilities	
Cloud Application Visibility	→ The Cloud Apps dashboard gives visibility into all sanctioned and unsanctioned cloud apps in use across the enterprise
Unsanctioned Cloud Application Blocking	→ Use web access controls to restrict access to unsanctioned cloud apps and shadow AI
Standard Compliance DLP	→ Protects sensitive info such as PII, PHI, PCI as well as password files and custom encrypted files from being sent over the web channel (for on-prem and hybrid this is provided via the Web DLP module, or integration with the full DLP Suite)
Forcepoint Data Security Integration	→ Easily inherit advanced data classifiers and DLP policies for use over the web channel with the click of a button
Threat Prevention Capabilities	
Proxy (SSL)	→ In-line inspection of all web traffic ensures maximum security efficacy
Real-time Security Classification	→ Employs many types of analysis to identify malicious code that is often hidden behind dynamic content
Real-time Content Classification	→ Classifies web content from any and all web pages into over 130 categories to enable highly granular access filtering
Anti-Virus, Anti-Malware	→ Applies state-of-the-art-malware protection capable of proactively blocking the latest in binary and script-based threats
Heuristic Analysis	→ To indentify and protect against malware that has not been encountered previously
Reputation Analysis	→ Reputation databases prevent traffic from being redirected to untrustworthy sites
URL Database	→ Classifies known URLs and assesses new URLs based on associated sites and redirections
Behavioral File Sandboxing	→ Advanced Malware Detection and Prevention (AMDP) adds the ultimate layer of security to ensure protection against zero-day threats nefariously hidden in files
Remote Browser Isolation	→ When the solution detects a risky site that should be blocked but the business needs to allow access anyways, the risky session can be handled via Remote Browser Isolation to ensure security while still permitting access
File Type Blocking (Inbound)	→ Allows blocking of inbound files based on file type within a policy
Cloud Application Risk Database	→ Identify the risk level of cloud apps that are being used across the enterprise
ThreatSeeker Global Threat Intelligence	→ Aggregates threat intel from Forcepoint products deployed around the world and provides threat telemetry back to all Forcepoint security solutions