Forcepoint ONE

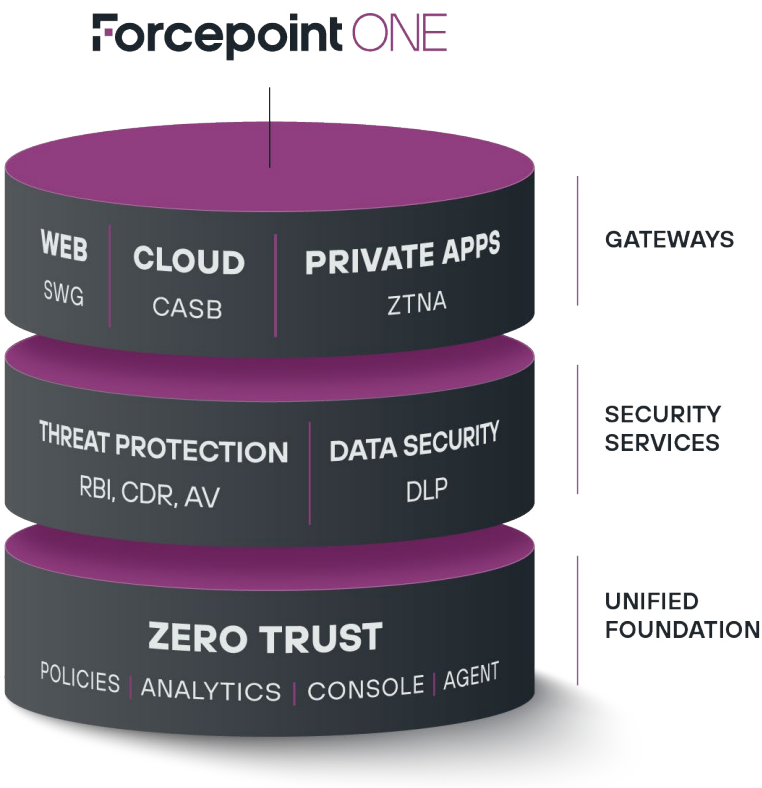
Forcepoint ONE is an all-in-one cloud service that makes security simple for distributed businesses and government agencies that need to adapt quickly to changing remote and hybrid workforces. It gives employees, contractors, and other users safe, controlled access to business information on the web, in the cloud (Saas and IaaS), and in private applications, while keeping attackers out and sensitive data in. As a result, Forcepoint ONE makes users more productive, whether remote or in the office, and businesses more efficient.

Key Benefits

- 99.99% verified uptime since 2015
- Latency minimized and throughput maximized with auto-scaling
- Flexible integration with any SAML-compatible IdP
- Unified administration console reduces repetitive and redundant configuration management
- Unified managed device agent for CASB, SWG, and ZTNA simplifies deployment
- AD sync agent or SCIM provisioning accelerate user on-boarding
- Reverse proxy with AJAX-VM allows protection of any managed web application without an on-device agent
- Data-in-motion scanning blocks malware and data exfiltration between users and any web application
- Data-at-rest scanning quarantines malware and controls risky data sharing for many popular SaaS and IaaS storage offerings
- Encryption of structured and unstructured data in SaaS and IaaS ensures data privacy
- Ability to block specific HTTP/S request methods, resulting in granular control of user interactions with any SaaS, web page, or private web application

Forcepoint ONE combines Zero Trust and SASE security technologies, including three secure access gateways and a variety of shared threat protection and data security services, all built on a cloud-native platform. This approach enables organizations to manage one set of policies, in one console, communicating with one endpoint agent.

- → **Secure Web Gateway (SWG).** Monitors and controls any interaction with any website, including blocking access to websites based on category and risk score, blocking download of malware, blocking upload of sensitive data to personal file sharing accounts, and detecting and controlling shadow IT. Currently available as agent software for Windows and MacOS.
- → **Cloud Access Security Broker (CASB).** Agent-based or agentless solution that enforces granular access to company SaaS based on identity, location, device, and group. Blocks download of sensitive data and blocks upload of malware in real time. Scans data at rest in popular SaaS and IaaS for malware and sensitive data and remediates as needed. Agentless option facilitates BYOD and contractor access.
- → **Zero Trust Network Access (ZTNA).** Agent-based or agentless solution that allows granular access to private applications without the use of a VPN. Agent based solution required for non-HTTP/S applications.



Common features for all three gateways include:

- → **Contextual access control.** Access to web, cloud, or private applications is controlled based on user location, device type, device posture, user behavior, and user group.
- → **Data loss prevention (DLP).** Files and text are scanned upon upload and download for sensitive data and blocked, tracked, encrypted, or redacted as appropriate.
- → **Malware scanning.** Files are scanned upon upload and download for malware and blocked when detected.
- → **Unified management console** for configuration, monitoring, and reporting.
- → **Unified on-device agent** for Windows and macOS.
- → **99.99% service uptime.**

Forcepoint ONE also includes these add-on capabilities:

- → **Cloud Security Posture Management (CSPM).** Scans AWS, Azure, and GCP tenant settings for risky configurations and provides manual and automated remediation.
- → **SaaS Security Posture Management (SSPM).** Scans Salesforce, ServiceNow, and Office 365 tenant settings for risky configurations and provides manual and automated remediation.
- → **Remote Browser Isolation (RBI) with integrated Content Disarm Reconstruction (CDR).** With the appropriate SWG content policy, a user is protected from web-borne malware on their local device by running a browser in a cloud-hosted VM. With CDR, document and image downloads can be stripped of embedded malware and reconstructed before being opened by a user. This includes removal of malware embedded in an image file using steganography.

Forcepoint ONE Features and Benefits

SCOPE	FEATURE	BENEFIT
Platform-wide	Auto-scaling, distributed architecture on AWS with over 300 POPs worldwide.	→ 99.99% uptime. → Minimal latency: often even faster than direct application access. → Faster scanning of data at rest: hours vs days to scan an entire application tenant's content.
	Integration with any SAML compatible IdP. SAML relay or ACS proxy mode. Optional built-in IdP using Microsoft ADFS.	→ Flexible deployment. → Denial of service protection when using SAML relay mode.
	Active Directory Sync Agent. Synchronizes your current AD users and groups with Forcepoint ONE users and groups.	→ Leverage your existing Microsoft AD instance to quickly onboard users and manage the groups they are in.
	SCIM Integration. Synchronizes your current Azure AD users and groups with Forcepoint ONE users and groups.	→ Leverage your existing Azure AD tenant to quickly onboard users and manage the groups they are in.
	Contextual access control. Grants user access to Forcepoint ONE based on user group, device type, location, or time of day. Optional escalation to Multi-factor Authentication based on "impossible travel," unauthorized location, or unknown device. Additional layer of access control for individual websites or applications based on user group, device type, or location.	→ Detecting and blocking suspicious login attempts reduces risks associated with stolen passwords. → Granular access control allows segmentation of users based on risk and need to access.
	Single unified agent for on-device SWG, CASB forward proxy, and ZTNA for non-web applications.	→ Simplified agent deployment including deployment through selected MDM systems. → Low CPU and memory. → Auto rotated, self-generated certificates ensure security and reduce IT overhead.
	Single administrator console for managing all system capabilities across all applications, users, and devices.	→ Single unified console reduces complexity and time to value while increasing visibility and control.
CASB, SWG, and ZTNA for web-based apps	DLP and malware scanning for data in motion. Scans file attachments downloaded from or uploaded to any web-based app or website for malware or sensitive data. Logs and takes the appropriate remediation action such as block (sole option for SWG), quarantine, encrypt, apply DRM, or apply watermarking and file tracking.	→ Reduces risk of data leakage and spread of malware in transit between users and any web application or website.
	Field Programmable SASE Logic. Monitors, logs, and optionally blocks any HTTP/S request method based on any portion of the request method.	→ More fine-grained control of app usage. → Ability to block upload of sensitive data as message posts.
CASB and ZTNA for web-based apps	Agentless reverse proxy with AJAX-VM. The reverse proxy is software running in our core and edge POPs, while the AJAX-VM is a Java Script abstraction layer running inside the end user browser. Both work together to ensure that Forcepoint ONE can manage traffic between any device and any managed web application, without the need for agent software running on the device.	→ Works with any web-based application including longtail and custom applications that other reverse proxy solutions cannot support. → No agent installation necessary for BYOD or contractors. → Works with any device supporting a modern browser.

SCOPE	FEATURE	BENEFIT
SWG	Monitors, logs, and controls access to any website from corporate Windows and Mac endpoints located anywhere with DLP and malware scanning using the Forcepoint ONE unified agent.	→ Enforces acceptable use policy. → Monitors shadow IT usage on managed devices. → Controls access down to the URL directory path level. → Blocks upload of sensitive data to any website. Blocks download of malware from any website. → Distributed enforcement architecture reduces traffic through the Forcepoint ONE backplane and results in near wire-speed throughput.
CASB	DLP and malware scanning for data at rest in the cloud. Scans structured and unstructured data in SaaS and IaaS storage for malware or sensitive data, and log and takes the appropriate protective action such as quarantine, encrypt, or remove public sharing.	→ Scans historical data not just recently added files. → Applies OCR to image files to detect sensitive text data. Turns off public sharing of files containing sensitive data. Quarantines malware stored in the cloud. → Extensive library of pre-defined data patterns reduces set-up time.
	Data Encryption. Encrypts sensitive structured and unstructured data in managed SaaS and IaaS.	→ Ensures sensitive data is only visible to authorized users.
	Shadow IT discovery and control	→ Use logs from corporate firewalls and proxy servers to discover shadow IT use. → Block users from using any shadow IT application while providing a coaching message recommending a company sanctioned alternative.
CSPM	Cloud Security Posture Management. Scans configuration of security settings for AWS, GCP, and Azure admin console SaaS in accordance with various industry and regional baselines as well as custom baselines.	→ Flags risky setting for remediation. Apply one-click remediation or automated remediation where applicable.
SSPM	SaaS Security Posture Management. Scans configuration of security settings for popular SaaS tenants in accordance with various industry and regional baselines as well as custom baselines.	→ Flags risky setting for remediation. Apply one-click remediation or automated remediation where applicable.
RBI with CDR	Remote Browser Isolation with Content Disarm and Reconstruction. A licensed option for Forcepoint ONE SWG. Provides a layer of abstraction by running a browser in a cloud-hosted VM, separating the end user device from the risk of web-borne malware. When the user downloads a document or image file, CDR is applied which extracts the valid business information from the file, verifies the extracted information is well-structured, and then builds a brand-new file to carry the information to its destination.	→ Web browsing experience is the same as it has always been. → Capable of rendering a broad set of web destinations—from modern cloud apps, like the Google Workspace, to sites built on legacy technologies. → Keeps sensitive web app data out of BYOD browser caches, limits website data sharing functions, and integrates with market leading DLP. → Files processed by CDR are malware-free. This includes removal of malware embedded in an image file using steganography.