Solution Brief

Forcepoint ONE: Cloud platform simplifies security for the hybrid workforce

Use Cases

- Gain visibility and control of hybrid workers' interactions with data in web, cloud, and private apps.
- Prevent misuse of sensitive data accessed from managed or unmanaged devices.
- Control access to high-risk web content.
- Provide remote, fast secure access to business resources and private apps without the complexity of VPNs.

Solution

- LA single, unified platform allows management of one set of policies across all apps, from one console through one endpoint agent.
- All-in-one cloud-delivered service that safeguards access and data by combining Secure Web Gateway (SWG) Cloud Access Broker (CASB), and Zero Trust Network Access (ZTNA).
- Integrated advanced threat protection and data security to keep attackers out and sensitive data in.
- Additional capabilities such as RBI with CDR for Zero Trust web access, CSPM for scanning public cloud tenants for risky configurations.
- Forcepoint Classification for data tagging, and others (see p. 2 for details).

Outcome

- Simplified – brings together security for web, cloud, and private apps into one set of policies, one console, one agent (with agentless support).
- Modern – combines Zero Trust principles with a SASE architecture and advanced security like Remote Browser Isolation and sanitizing of downloaded files.
- Everywhere – is available globally, with more than 300 points of presence (PoPs).
- Reliable – delivers verified 99.99% uptime since 2015.
- Fast – uses distributed enforcement and automatic scaling to eliminate choke points.

Data-first Security

Security keeps getting more complex, but there is a better way. Users are now working from anywhere with data that is spread everywhere—in websites, cloud apps, and private apps.

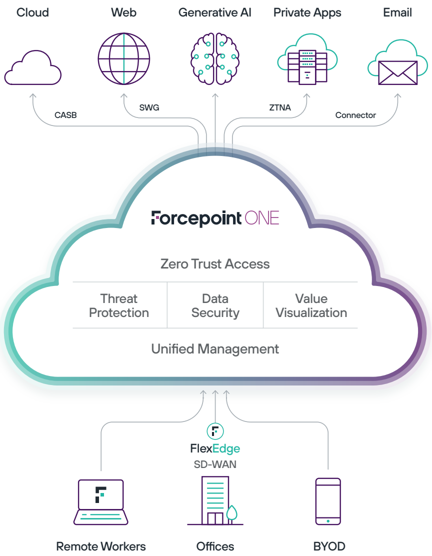
In order to support return to office (RTO) initiatives and hybrid workforces security teams need a converged security platform that puts data at the center of the picture. Security controls need to be able to extend across web, cloud, and private app access with consistent visibility and control so organizations can move left of loss to stop data loss before it occurs.

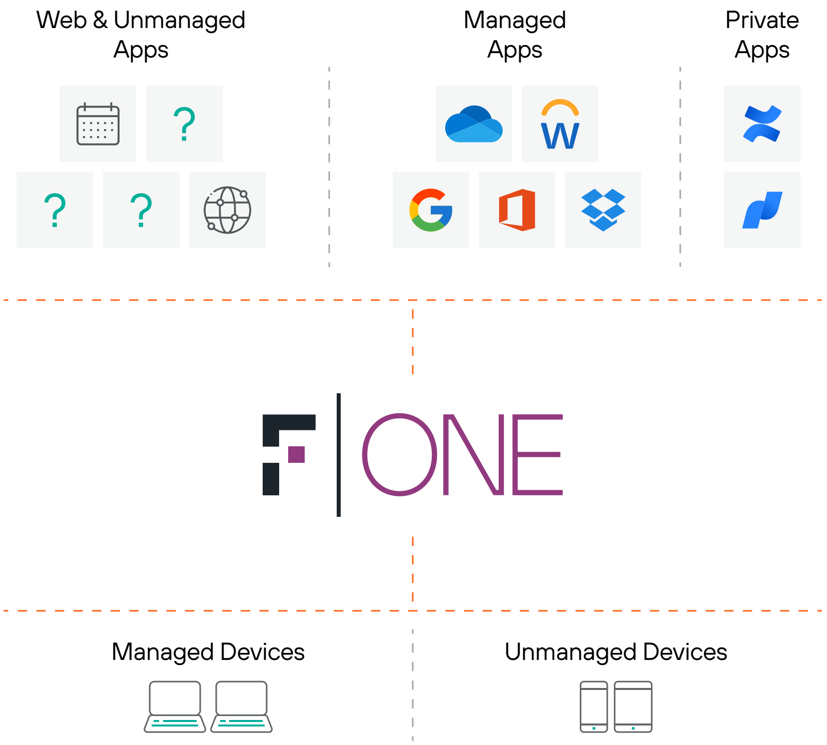
With a data first solution business data can be secured everywhere for people working anywhere.

Forcepoint ONE Simplifies Security

Forcepoint ONE is an all-in-one cloud platform that makes security simple. You can quickly adopt Zero Trust and Security Service Edge (SSE, the security component of SASE) because we unified crucial security services, including Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) and Zero Trust Network Access (ZTNA).

No more fragmented products. We give you one platform, one console, and one agent, with many solutions. Gain visibility, control access, and protect data on managed and unmanaged apps and all devices, from one set of security policies.





Secure data everywhere, for people working anywhere

The cloud-native, Zero Trust capabilities of Forcepoint ONE include:

- → **Agentless DLP security for cloud and private apps.** Safely use private business web apps from personal devices, while keeping sensitive data secure.
- → **Integrated advanced threat protection and data security.** across all gateways prevent data loss or exfiltration and stop hackers from getting in.
- → **Unified gateways for cloud, web, and private app access.** Identity-based access control to business apps managed in one place for SWG, CASB, and ZTNA.
- → **Dynamic scalability with global access.** 300 PoPs built on AWS provide fast, low-latency connectivity and 99.99% uptime regardless of where people work.

Unified security for web, cloud, and private apps

- → **Cloud:** CASB enforces granular access to corporate SaaS apps and data from any device. CASB blocks download of sensitive data and blocks upload of malware in real time. It scans data at rest in popular SaaS and IaaS for malware and sensitive data and remediates as needed. CASB detects shadow IT apps and controls access from any managed device.
- → **Web:** SWG monitors and controls interactions with any website based on risk and category, blocking download of malware or uploads of sensitive data to personal file sharing and email accounts. Our ondevice SWG enforces acceptable use policies on managed devices located anywhere.
- → **Private apps:** ZTNA secures and simplifies access to private applications without the complication or risk associated with VPNs.

Pervasive data security and threat protection

→ **Data Loss Prevention (DLP):** Files and text are scanned upon upload and download for sensitive data and blocked, tracked, encrypted, or redacted as appropriate. Over 190 predefined DLP rules help to streamline regulatory compliance and provide quick time to value. Easy integration with Forcepoint Enterprise DLP enables data security everywhere—on the endpoint, in the network, on the web, and in cloud services.

→ **Malware scanning:** Files are scanned upon upload and download for malware and blocked when detected.

Simplified enforcement from a single set of policies

→ **Single management console** for configuration, monitoring, and reporting.

→ **Single set of login policies** for controlling access to web, cloud, or private applications based on user location, device type, device posture, user behavior, and user group. These parameters help prevent account takeovers.

→ **Single set of DLP policies** for controlling download and upload of sensitive data and malware for managed SaaS apps, private apps, and websites, as well as for data stored in managed SaaS and IaaS.

→ **Unified on-device agent** for Windows and MacOS for supporting SWG, CASB, and ZTNA for nonbrowser client apps and shadow IT control.

→ **Unified analytics and value visualization** for quick insights into security risks, overall utilization, and impact of the all-in-one cloud security platform.

Additional capabilities available as needed

→ **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):** Protects a user from web-borne malware on their local device by running a browser in a cloud-hosted VM. Uses CDR to sanitize files downloaded during an RBI session of any malware or foreign elements.

→ **Forcepoint Classification:** Data classification tagging with AI powered suggestions to enhance tagging accuracy.

→ **Cloud Firewall:** Add-on to SWG to secure all internet traffic and safeguard against attacks designed to exploit vulnerable branch sites.

Subscriptions that unlock simplicity

Annual subscriptions per-user are available:

→ **All-in-one edition** for web, cloud, and private app security.

→ **Web-security edition** includes the web gateway plus inline CASB for unlimited cloud apps, and allows customers to add API support for cloud apps and support for private apps later.

→ **ZTNA edition** protects an unlimited number of private applications.

→ **CASB edition** protects an unlimited number of cloud applications inline, and includes APIs for 3 applications with the ability to add additional app packs or dedicated API polling nodes.

→ **All subscriptions** include centralized cloud management, unified policies with data loss prevention, automated access via a unified endpoint agent, and comprehensive reporting.

forcepoint.com/contact