Forcepoint

Solution Brief

Zero Trust Network Access

Simplify security for private apps without a VPN

Use Cases

- Replace VPNs for accessing private apps in data centers and private clouds.
- Provide safe, agentless access to private web apps from BYOD and unmanaged devices.
- Control uploading and downloading sensitive data in any private web app.
- Stop malware hidden in business data files to and from private web apps.
- Safeguard access to private non-web servers from managed Windows and macOS devices.

Solution

- Private app security integrated with advanced threat protection and DLP.
- Agentless, Zero Trust access controls for private web apps from BYOD and managed devices.
- Remote access to non-web private apps from managed Windows and macOS devices.
- Part of an all-in-one cloud-delivered service with SWG, CASB, and other modern security capabilities.

Outcome

- Increase productivity, enabling people to access private apps seamlessly and safely from anywhere.
- Reduce costs by simplifying security operations with a single place to set policies.
- Reduce risk through control of sensitive data and malware in transit to and from private web apps.
- Streamline compliance with demonstrable processes for controlling information.

Remote work has exposed the limitations, costs, and risks of virtual private networks (VPNs). Once connected, VPNs grant excessive implicit trust, letting users scan and probe other IP addresses in that private data center or virtual private cloud, which opens the door to breaches. However, enterprises that want to move on from VPNs to Zero Trust Network Access (ZTNA) solutions should not have to face more complications and point products; the adoption of Zero Trust access should be simple and smooth.

The ZTNA from Forcepoint controls access to private web and non-web apps that each employee, contractor, and partner has explicit permission to use. Forcepoint ZTNA gives you infinitely greater control with the confidence to allow people to use the devices that work best for them, even unmanaged devices and BYOD.

Unlike other solutions, Forcepoint ZTNA also delivers continuous, fine-grained controls, industry-best performance, and built-in malware and data protection to offer a great user experience despite the intricacies of modern networks. You can also easily add other security solutions like Cloud Access Security Broker (CASB) and Secure Web Gateway (SWG) as needed, fully integrated as part of Forcepoint ONE cloud platform.

Replace VPNs for accessing private apps in data centers and private clouds
Secure access to private apps is about fast, pinpoint control. You can limit access to private apps like ERP or supply chain servers based on identity, group membership, device type and location. For non-web apps, you can apply controls per port and protect access from unknown locations or devices. If the login attempt looks suspicious, users must prove their identity through multi-factor authentication (MFA). All of this happens in milliseconds with Forcepoint's hyperscale platform.

Provide safe, agentless access to private web apps from BYOD
Users can safely and conveniently connect over the internet to web apps hosted behind a firewall, even from BYOD and unmanaged devices, without needing agents.

Control uploading and downloading of sensitive data in any private web app
Manage one set of security policies to control sensitive data, with access to malware-scanning and DLP built-in to stop hackers and data breaches. Combining data security with policies for device posture and location makes it easier to control how people move data from and to private web apps on any device.

Stop malware hidden in business data files to or from private web apps
Forcepoint curbs ransomware. Detect and block malware in data-in-motion between users and any private web app using Bitdefender and CrowdStrike scanning engines.

Safeguard access to private non-web servers from managed devices

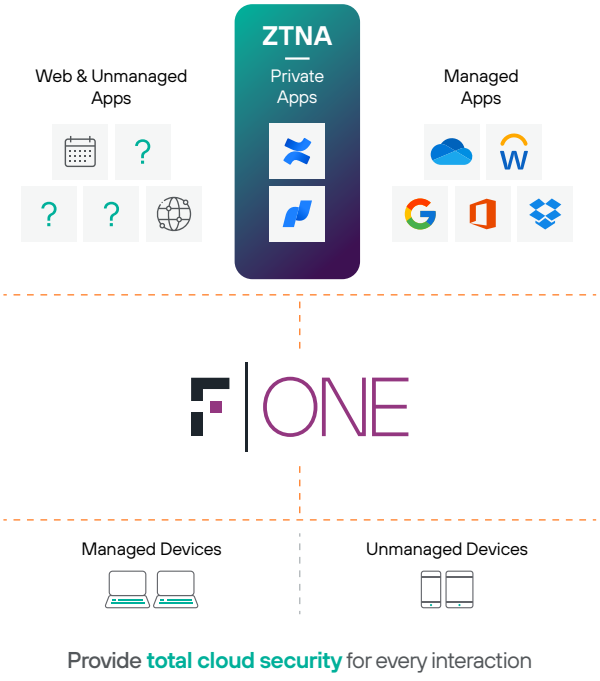
Our ZTNA enables access to private non-web apps like secure shell (SSH) and remote desktop from managed PCs or Macs with the Forcepoint ONE unified agent.

ZTNA in Forcepoint ONE maximizes uptime, availability, and productivity

ZTNA is part of Forcepoint ONE, our hyperscaler-based cloud platform with 300 points of presence (PoPs), global accessibility, and proven 99.99% uptime to secure private apps seamlessly and preserve user productivity. Other solutions detour network traffic through private data centers instead of locations close to users, which can create poor performance. Forcepoint ONE unifies CASB, SWG, and ZTNA to secure access to corporate SaaS, web, and private apps, making security simple.

Making Private App Security Simple in the Real World

The Forcepoint ONE cloud platform provides an "easy button" for implementing private app security. From one console, administrators can manage access and control file downloads and uploads for users of both managed and unmanaged devices (such as BYOD and contractors' or partners' computers).



Provide **total cloud security** for every interaction

Let's see how the ZTNA capability simplifies private app security when Kris, a purchasing manager working from home, starts their day.

Kris logs into his Forcepoint ONE account from his corporate-issued laptop.	Since Kris is trying to log in from a managed device, and from a permitted location, they are granted access. A login attempt from an unknown location requires a successful response through MFA apps.
Kris gets one-click access to the company's proprietary supply chain application from the Forcepoint ONE user portal.	Kris' browser displays the Forcepoint ONE portal, showing tiles for each web app Kris and their supply chain partners can access. (If Kris' company uses Forcepoint ONE CASB, Kris' managed SaaS apps are accessible from the same user portal for a consistent experience.)
Kris is granted managed app access.	Traffic between Kris' laptop and the supply chain app automatically passes through the Forcepoint ONE reverse proxy. Forcepoint scans file uploads and downloads for malware and sensitive data.
Kris uploads a vendor contract as an attachment.	Since the policy for Kris' connection specifies scanning files, the upload is allowed if the file is malware-free. If it is infected, the ZTNA gateway blocks the upload, alerts Kris, and logs and reports the block event.

Part of a unified security solution for web, cloud, and private apps

In addition to ZTNA, the Forcepoint ONE all-in-one platform secures access to business information on any website and private app:

- → **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 on-device SWG enforces acceptable use policies on managed devices anywhere.
- → **Cloud:** CASB secures and simplifies access to corporate SaaS and IaaS tenants while controlling the transmission of sensitive data and malware, without the need for an on-device agent.
- → **Additional capabilities** such as RBI or scanning cloud providers for risky configurations (CSPM) as needed.

Read the Forcepoint ONE Solution Brief for more details.

Ready to secure data in cloud apps from any device?

Let's start with a demo.

forcepoint.com/contact