Forcepoint

FileOrbis Integrated

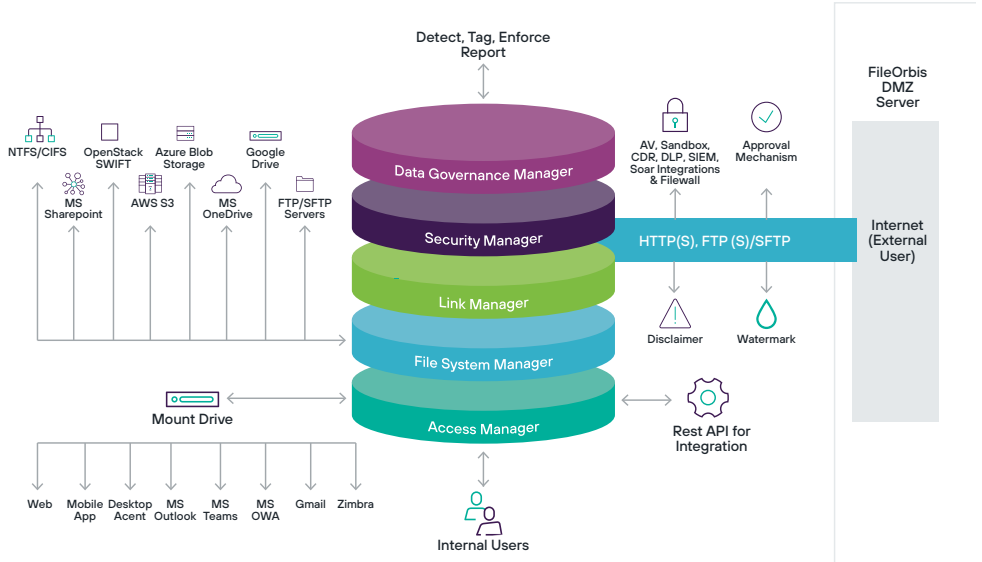
with Forcepoint

Key Benefits:

- **Increased accessibility and security** for all file repositories
- **Easy file sharing** between internal and external stakeholders
- **Control** over BYOD devices
- **Provide an extra layer of security** to file sharing with Forcepoint DLP
- **Sanitize uploads and downloads** with Forcepoint CDR API
- **Ensure balance** between security and productivity
- **Enhance productivity** in hybrid workplaces
- **Data-in-motion scanning** blocks malware and data exfiltration between internal and external users
- **Apply OCR to image files** to detect sensitive text data

The Challenge

As an impact of the digital era, information can be found anywhere. Employees may need to access company data from outside of traditional office buildings due to factors such as working from home, remote office scenarios, a highly distributed workforce, etc. This makes the issue of how to access and share content in a secure and user-friendly way a crucial one for companies. Files submitted for secure content sharing must first pass the security checks set forth by the organization's standards. The standards established while carrying out these procedures should not cause disruption to business units and processes.



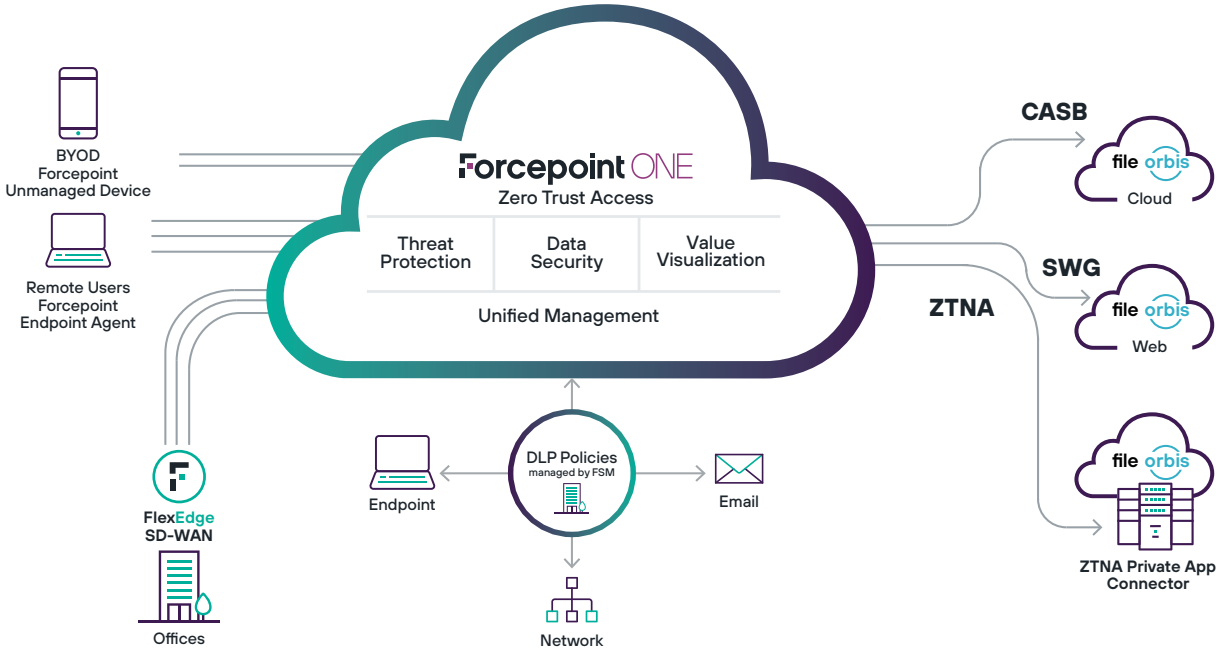
The Solution

Instead of directly accessing FileOrbis, Forcepoint ONE has implemented a SAML integration with two purposes: enhancing accessibility and bolstering security. By utilizing this integration, users can access applications through the powerful frameworks of agent-based or agentless Secure Web Gateway (SWG), Zero Trust Network Access (ZTNA) and Cloud Access Service Broker (CASB). These frameworks are meticulously orchestrated by Forcepoint ONE's comprehensive rule set, ensuring a robust and secure user experience.

In addition, the SAML integration implemented by Forcepoint ONE incorporates the Forcepoint DLP SSE Apps (Forcepoint Enterprise DLP) to ensure the integrity of data during the file upload and download processes. This integration enables organizations to securely share files while adhering to their data security policies. By leveraging Forcepoint DLP and the seamless integration via the Forcepoint DLP SSE app, organizations can protect the confidentiality, integrity and availability of their valuable assets.

To address the evolving landscape of advanced threats, an extra layer of security is necessary. The Forcepoint Zero Trust Content Disarm & Reconstruction (CDR) API seamlessly integrates during both file upload and download procedures. This integration effectively sanitizes and eliminates any potential malicious elements from files using advanced threat intelligence.

Forcepoint ONE incorporates multiple robust malware protection modules. By integrating cutting-edge technologies, Forcepoint ONE offers unparalleled defense against advanced threats. Incorporating these modules into the upload and download workflows allows organizations to operate in a secure environment, safeguarded against sophisticated malware, and effectively mitigate risks.



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.

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.

The **Secure Web Gateway (SWG)** monitors and controls any interaction with any website, including restricting access to websites based on category and risk score, preventing downloading of malware, blocking uploading of sensitive data to personal file sharing accounts, and detecting and controlling shadow IT. It is currently available as agent-based software for Windows and macOS.

The **Cloud Access Security Broker (CASB)** is an agent-based or agentless solution that enforces granular access to company SaaS based on identity, location, device and group. It blocks downloading of sensitive data and uploading of malware in real time. The CASB scans data at rest in popular SaaS and IaaS applications for malware and sensitive data and remediates as needed. The agentless option facilitates BYOD and contractor access.

Zero Trust Network Access (ZTNA) is an agent-based or agentless solution that allows granular access to private applications without the use of a VPN. The agent-based solution is required for non-HTTP/S applications.

Common features for all three gateways include:

→ Contextual access control

→ Data Loss Prevention (DLP)

→ Malware scanning

→ Unified management console

→ Insights analytics dashboards

→ Unified on-device agent

→ 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 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 Data Classification** tagging with AI-powered suggestions to enhance tagging accuracy.

About FileOrbis

FileOrbis is a platform for managing various aspects of the file environment, such as user profile folders, user-specific areas and network disks. It aids businesses at any stage in content management and from any angle, including but not limited to access and authorization management, file sharing, logging and more. FileOrbis integrates with security and content analysis solutions, allowing you to run all file environments concurrently and/or in series more securely and effectively.

FileOrbis Contact

Barbaros Mah. Kardelen Sk. Palladium Tower No:2 Ataşehir İstanbul
+90 (850) 885 0005 info@fileorbis.com
www.fileorbis.com

FileOrbis allows you to:

→ Resolve your cloud-based unchecked file sharing problems with support for HTTP(S), FTP(S) and SFTP protocols.

→ Solve your external file access and VPN management problems.

→ Solve the problem of failing to send email attachments and email servers' running out of space due to attachments.

→ Solve your access reporting and log problems in all file environments.

→ Eliminate the permission complexity and unused files on file servers.

→ Solve access and permission management problems. Generate user- and user group-based special access policies.

→ Create public workspaces.

→ Contribute to your legal requirements such as KVKK and ISO 27001.

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

forcepoint.com/contact

Forcepoint

[FP-FileOrbis-Integrated-with-Forcepoint-Flyer] 25Oct2023